

**H2020 – BES – 5 – 2015**

**Research Innovation Action**



**Intelligent Portable ContROl SyStem**



*This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700626*

## D 1.2 OEI – Requirement No. 2

Report Identifier:	D1.2		
Work-package, Task:	WP1	Status – Version:	1.00
Distribution Security:	CO	Deliverable Type:	R
Editor:	LUH		
Contributors:	LUH		
Reviewers:	[REDACTED] (Ethical Advisor)		
Quality Reviewer:	ED		
Keywords:			
Project website: <a href="http://www.iborderctrl.eu">www.iborderctrl.eu</a>			

### **Copyright notice**

© Copyright 2016-2019 by the iBorderCtrl Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

## Table of Contents

<b>ABBREVIATIONS.....</b>	<b>5</b>
<b>1 EXECUTIVE SUMMARY .....</b>	<b>7</b>
<b>2 INTRODUCTION.....</b>	<b>8</b>
2.1 SCOPE AND MAIN OBJECTIVES OF THIS DELIVERABLE .....	8
2.2 STRUCTURE OF THIS DOCUMENT .....	9
<b>3 METHODOLOGY.....</b>	<b>10</b>
3.1 ETHICAL RISKS AND THE DIFFERENT PHASES OF IBORDERCTRL .....	10
3.2 INTERRELATION OF D1.2 WITH OTHER TASKS.....	11
<b>4 ETHICAL CONCERNS WITH REGARD TO IBORDERCTRL.....</b>	<b>13</b>
4.1 RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA.....	13
4.2 UNEQUAL TREATMENT.....	15
4.2.1 Legal Background .....	15
4.2.2 Introduction .....	15
4.2.2.1 Legal sources of non-discrimination and equality.....	15
4.3 HUMAN DIGNITY.....	17
4.3.1 Legal Background .....	17
4.3.1.1 Introduction.....	17
4.3.1.2 Legal Sources of Human Dignity.....	17
4.4 RISK OF STIGMATIZATION AND THE IMPACT OF TECHNOLOGY.....	19
4.4.1 Definition and Classification of False Positives & False Negatives in the Legal Framework.....	19
4.4.2 Ethical implications of false positives .....	20
4.4.3 Impact on the Individual vs. Impact on Other Travellers.....	20
4.4.4 Data Quality and Falsified Information.....	22
4.5 PROFILING OF TRAVELLERS .....	23
4.5.1 Proposed Risk Indicators.....	24
4.5.2 Proposed risk thresholds.....	28
4.6 AUTOMATED DECISION MAKING .....	29
4.7 IMPACT OF HUMAN-MACHINE INTERACTION .....	31
4.7.1 Degradation of the Traveller to an Object.....	31
4.7.2 Cultural and Religious Implications .....	32
4.7.3 Questions asked during the Avatar Interview .....	32
4.8 FUNCTION CREEP .....	33
<b>5 CONCEPT OF INFORMED CONSENT .....</b>	<b>34</b>

---

5.1	GENERAL PRINCIPLES.....	34
5.2	ETHICAL ISSUES REGARDING THE EFFECTIVENESS OF MEASURES BASED ON INFORMED CONSENT .....	39
<b>6</b>	<b>RISK MITIGATION PLAN.....</b>	<b>41</b>
6.1	RESEARCH PHASE.....	41
6.1.1	Overall Design of the Test Pilots .....	41
6.1.2	System requirements .....	41
6.1.3	Anonymisation and Pseudonymisation.....	42
6.1.4	Transparency and Training .....	42
6.1.5	Legal obligations for all parties involved.....	43
6.2	EXPLOITATION PHASE .....	43
<b>7</b>	<b>CONCLUSIONS .....</b>	<b>45</b>

## Abbreviations

ADDS	Automatic Deception Detection System
approx.	approximately
Art.	Article
BCP	Border Crossing Point
BVerfG	Bundesverfassungsgericht (German Constitutional Court)
BVerfGE	Sammlung der Entscheidungen des BVerfG (German Constitutional Law Gazette)
BvR	File Number for Constitutional Complaint, German Constitutional Court
CFREU	The Charter of Fundamental Rights of the European Union
CIRAM	Common Integrated Risk Analysis Model
DoW	Description of Work
e.g.	<i>exempli gratia</i> – for example
EC	European Council / European Community
ECHR	European Court of Human Rights
ECR	European Court Reports
EEA	European Economic Area
EES	Entry/Exit System
EJIL	European Journal of International Law
Etc.	Et Cetera
ETS	European Treaty Series
EU	European Union
EUROPOL	European Police Office

FADO	False and Authentic Documents Online
FRONTEX	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
Ibid	<i>Ibidem</i> – in the same place
iBorderCtrl	Acronym for the project “Intelligent Portable ContROl SyStem”
ID	Identity document
i.e.	<i>Id est</i> – it is
iFADO	Intranet of False and Authentic Documents Online
INTERPOL	International Criminal Police Organization
IT	Information Technology
LUH	Leibniz University Hanover
MS	Member State
No.	Number
NVB	Non Verbal Behaviour
p.	page
RBAT	Risk-Based Analytics Tool
Rn.	Randnummer
SBC	Schengen Borders Code
UDHR	Universal Declaration of Human Rights
v.	<i>versus</i>
Vol.	Volume

# 1 Executive Summary

The EU external border control (Schengen Agreement) has recently become an issue of public debate largely due to the influx of migrants and refugees coming to the EU from war-torn regions, in particularly the Middle East. The EU has attempted to manage this challenge in several ways and overall the right to control the (Schengen) borders has been exercised. Furthermore, this was done inter alia, through initiating some new regulations and/or amending existing ones. For example, a recent change in the Regulation (EU) 2016/399 amended by Regulation (EU) 2017/458 meant that all travellers would undergo assessment and systematic check irrespective of whether they are EU citizens or third country nationals. Additional reforms such as the Smart Border Package shows the efforts at EU-level. While effective border control seems to require innovative technologies as proposed in the iBorderCtrl, it shall be mentioned that various legal and ethical issues need to be clarified for their effective and lawful implementation. Especially where such technologies are not covered by an existing legal basis it is vital to ensure legal and ethical compliance and two very basic interests must be weighed against each other; on the one hand, there is a need to ensure effective border checks, on the other it is vital to protect travellers' privacy and other fundamental (human) rights. To achieve legal and ethical compliance the project and the technology proposed has been carefully analysed and made subject of two deliverables. D2.3 and 1.2.

D2.3 consists of several sections discussing the identified legal issues. First, the different components of the iBorderCtrl toolkit are described in order to note the status of the technical components on which basis the legal analysis is conducted at this stage of the project. Second, the legal framework is described in order to provide an overview of the different laws that should be considered, and how they interact with each other. In a third step, the technical descriptions are subsumed under the current legal framework.

D1.2 deals with the ethical implications of the project. Whilst there are necessary and unavoidable overlaps between the legal and the ethical deliverable, it was the aim of 1.2 to more thoroughly analyse the ethical and moral rights implications of the project that have been identified in D2.3. After an introduction to the ethical issues at hand, the issue of unequal treatment and the element of human dignity will be elaborated. After that particular ethical / philosophical risks that have been identified in D2.3 will be further elaborated. Firstly, there is a risk of stigmatisation, which is inter alia associated with data accuracy and quality depending on the data sources used to calculate the risk scores. There is a risk of false positives and negatives which needs to be addressed. Secondly, and closely connected with the risk of stigmatisation, issues raised by profiling of travellers needs to be addressed. Thirdly, another issue is automated decision making in which context the issue of algorithm bias also needs to be addressed. Furthermore, there are concerns that relate to the impact of human machine interaction. Finally, ethical considerations in the context of informed consent need to be addressed as iBorderCtrl relies on consents as legal justification to process personal data, both during the research phase as well as afterwards in a possible exploitation scenario, it is an ethical question to what extent informed consent may serve as a legal basis.

## 2 Introduction

Controlling the EU external borders has become an issue of intense discussion. The overarching policy is that EU and its Member States have the right to control their borders. Constant legal reforms are being witnessed as the Schengen acquis has gone through considerable amendment. In this regard, various topics related to migrant control, in particular the refugee crisis and the threats for public security caused by terrorism, increase the pressure on the European legislator to find remedies. Fostering more efficient border controls, mainly by substituting the current system with new technologies and/or functionalities, is one aspect which appears to be of particular interest. In December 2016, the European Commission published a proposal on how to reinforce the Schengen Information System to better fight terrorism and cross-border crime, proposing changes such as improving the security and accessibility of the system, introducing the obligation to create a SIS alert in cases related to terrorist offences or improving information sharing and cooperation between Member States, notably through the introduction of a new alert category on "unknown wanted persons" and full access rights for Europol.<sup>1</sup> In May 2017, the Commission set out a new approach on interoperability of information systems by providing a European search portal, a shared biometric matching service and establishing a common identity repository.<sup>2</sup> This very much shows that new technologies regarding innovative means of collecting, processing and sharing electronic information (including personal data) can and will be utilised for border checks. While the border is the gateway to controlling movement and other activities that may affect public security, border control activities are nevertheless subject to certain rules of international and national law. In particular, international law imposes duties on the state not to carry out their border control exercises in a manner that may violate human rights. To this extent, the fundamental human rights to human dignity, equality and privacy are of particular importance within the scope of iBorderCtrl.

A specific challenge in this regard is the lack of coverage of existing regulations to these new technologies. In fact, this gap usually results in certain questions: How do these new developments fit into the current legal framework, and which moral principles form the basis of the current legislation? Will these moral principles allow extending the scope of the existing legal provisions to the application of new technologies? What are the benefits and risks, both for the individual as well as the society? The emergence of new technologies that require processing of personal data increase privacy risks and consequently require appropriate legal and ethical safeguards to counterbalance the need for an efficient border control against the protection of the individual's rights and thus ensuring that high morale standards are being observed.

### 2.1 Scope and main objectives of this deliverable

This deliverable will focus on ethics of profiling and the risk of stigmatization of individuals and groups. The general outset for this deliverable will be outlined in the legal review being performed within Task 2.3, and follow-up on particular ethical concerns identified therein. In particular, the risks arising from false positives need to be tackled in order to ensure that individuals are not discriminated due to technical malfunctions or computer-based or computer-aided decisions.

Ethics can be seen as a set of morale principles inherited by the society and the legal framework. Many of those principles are stipulated in fundamental human rights, such as the right to human dignity,

---

<sup>1</sup> [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication\\_eas\\_progress\\_since\\_april\\_2015\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf).

<sup>2</sup> [http://europa.eu/rapid/press-release\\_IP-17-1303\\_en.htm](http://europa.eu/rapid/press-release_IP-17-1303_en.htm).



equality and non-discrimination. These rights may be only restricted by law if any other fundamental human rights, such as the right to physical integrity and life, in the context of iBorderCtrl in the light of public security, are affected. In such cases, the principle of proportionality requires the law to balance out conflicting interests, ensuring that any restrictions are based on morally sound decisions. With regard to iBorderCtrl, the very first step to allow an ethical assessment is to define the conditions under which a sub-system might cause certain ethical challenges. Following the legal principles inherited in the European legal system, ethical issues potentially arise if

- a person's fundamental human rights are affected,
- there is no legal basis that (clearly covers) the use of such technology and
- the circumstances under which such technology is used differs from the status-quo

This being said, it has to be noted that the ethical report will not focus on all potential conflicts of fundamental rights – this would be subject to respective jurisdiction - but rather on technological developments that might impact the society and technological realities on a larger scale.

## 2.2 Structure of this document

The ethical report will be structured as follows:

- Section 3 will describe the methodology on which this report is based upon. In particular, it will describe the approach to ethical issues and the interrelation with the legal report. This shall provide a better understanding of how legal and ethical issues are interlinked and how ethical compliance may be ensured in iBorderCtrl.
- Section 4 will focus on aspects and functionalities that are of particular importance from an ethical point of view. The topics that are of particular relevance from an ethical point of view have been identified within the scope of Task 2.3.
- Section 5 will focus on the doctrine of informed consent, its ethical ramifications and how this concept can be utilised within the scope of iBorderCtrl. To this extent, not only the requirements for obtaining informed consent will be described, but also the different risks that can arise from an ethical point of view, both for the research phase as well as the exploitation phase of iBorderCtrl.
- Section 6 will include a risk mitigation plan aiming at avoiding ethical risks for participants of the test pilots and travellers. As the risk mitigation plan was implemented in the reference architecture D2.2, a particular focus was put on measures that could be implemented in the architecture of iBorderCtrl.
- Section 7 concludes this report, providing a summary of the major findings of this deliverable, as well as suggestions to ensure high standards with regard to ethical issues.

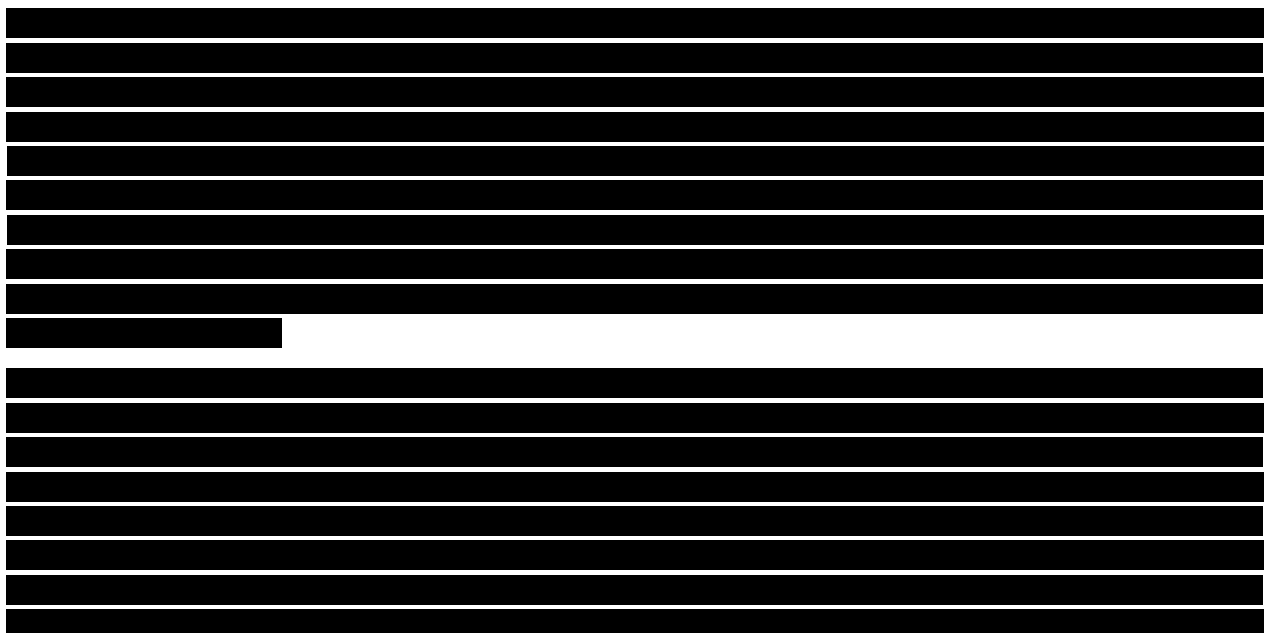
### 3 Methodology

A necessity of iBorderCtrl is that all aspects of the project — the toolkit which is being developed as well as all actions in the research, development or deployment and the use of the iBorderCtrl platform — shall be compliant with the current legal framework and the underlying moral principles. This requires a detailed analysis on the different ethical implications and options to mitigate such risks for the individual. A major challenge in this regard is that iBorderCtrl provides complex technical requirements while it is still in a very early project phase, and details on certain functionalities or usable prototypes are not yet available as this document is written.

Given the foregoing, this deliverable seeks to provide an overview of the ethical challenges and possible measures to mitigate such challenges. To achieve this goal, the following methodology shall apply:

- Firstly, the ethical research is closely interlinked with other tasks of the project, in particular with the legal analysis conducted in D2.3. To this extent, D2.3 constitutes the basis of this report, as both the overall legal framework and the technologies adopted in iBorderCtrl are crucial aspects in order to identify ethical challenges.
- Secondly, the ethical report, as well as the legal analysis, distinguishes between the two phases of iBorderCtrl – the development of the tools including the test run and the exploitation. This is particularly important, as risks for individuals may change with regard to the different aims and applications of the iBorderCtrl toolkit in each phase.
- Based on the ethical issues identified, risk mitigation measures and further propositions to ensure high ethical standards will be explored and developed. In this regard, the impact of the various technologies developed in iBorderCtrl, how they will be used and how far they will change or complement the current system of border checks will be assessed. In order to supplement the identification of ethical issues and the implementation of mitigation measures.

#### 3.1 Ethical risks and the different phases of iBorderCtrl



[REDACTED]

[REDACTED]

### 3.2 Interrelation of D1.2 with other Tasks

[REDACTED]

[REDACTED]

[REDACTED]

- 
- [REDACTED]
  - [REDACTED]

---

[Redacted content]

#### 4 Ethical concerns with regard to iBorderCtrl

[illegible]

#### 4.1 Right to Privacy and Protection of Personal Data

Privacy and data protection is a pivotal point and became a priority for policy makers and European interlocutors to shape the future of the information society and smart products and devices. Thus, and given the prominence of the issue, the technical and legal development must be reconciled with ethical / philosophical considerations, since the development and adaption of ethical principles has for the most parts been concurrent with the development of law in the field. The ethical foundations of the concept of privacy can be traced back to ancient times, since the earliest surviving version of the Hippocratic oath included the phrase: "And whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."<sup>5</sup> A more recent publication on the concept of privacy and seminal theoretical contribution certainly is Warren and

<sup>5</sup> Hippocrates of Cos, "The Oath". Loeb Classical Library (1923) 147: 298–299. doi:10.4159/DLCL/hippocrates\_cos-oath.1923. last accessed on

Brandeis' legal and ethical considerations of the right to privacy in 1890.<sup>6</sup> It is not merely a coincidence that the text was written in times of radical change, acceleration of life, industrial production and the distribution of information via telephone or radio broadcast. Just like at the beginning of the 20<sup>th</sup> century we find ourselves in the middle of dramatic changes, where artificial intelligence, the Internet of Things, Smart Traffic and Big Data create opportunities that were still inconceivable some years ago. All the advantages of modern information technologies, however, cannot conceal the fact that there are disadvantages and risks as well and we are already at a point where traditional concepts of privacy and its ethical /philosophical fundament dealing with the vulnerabilities of persons in digital societies seemingly require sensible adjustments. Privacy, the protection of personal information and its philosophical justification after all remains a complex issues, due to its interrelation to various other areas of law and philosophy dealing with the protection of individuals.

The CFREU contains several privacy and data protection related provisions which are relevant in the context of iBorderCtrl. Art. 7 (Respect for private and family life) reads: "Everyone has the right to respect for his or her private and family life, home and communications" Furthermore Art. 8 (Protection of personal data) stipulates that "Everyone has the right to the protection of personal data concerning him or her".<sup>7</sup> And Art. 8 (2) CFREU determines that personal "data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."

The right to privacy also does exist on EU- member states level as numerous constitutions implicitly or explicitly grand or respect the right to privacy. In the case of Germany for instance the German Federal Constitutional Court interpreted that the German Constitution ("Basic Law") includes a right to "informational self-determination" derived from Art. 1(1), 2(1) Basic Law. The term was first used in a German constitutional ruling in connection with personal information collected during a census in 1983. In particular the German Constitution Court held that "... in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution. This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data. Limitations to this informational self-determination are allowed only in case of overriding public interest."<sup>8</sup>

Because of this, we shall in the following further discuss the underlying ethical and philosophical implications of privacy as well as aspects of fundamental rights implications relevant in the context of iBorderCtrl. Most prominently and also closely connected with the ethical / philosophical foundation of privacy are the issues of equality or equal treatment and human dignity.

---

<sup>6</sup> Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5 (1890), pp. 193-220.

<sup>7</sup> Art. 8 (1) CFREU

<sup>8</sup> In German: BVerfGE 65, 1 - Volkszählung

## 4.2 Unequal Treatment

### 4.2.1 Legal Background

Although this deliverable has an ethical focus, it must be borne in mind that ethical considerations may (or should) also be tested against a legal background; that, in other words, ethical considerations may considerably overlap with a legal fundament and constitutional framework.

### 4.2.2 Introduction

The concept of equality and non-discrimination are very complex concepts with numerous ramifications and consequences. This topic is both challenging from a legal as well as an ethical point of view and leaves room for considerable debate over the meaning and its justification.

Therefore, we shall first explain the legal background and from there will explain and develop the meaning of equality or equal treatment and/or its antagonist inequality or unequal treatment. In the context of the project iBorderCtrl, it is vital to have a sound understanding of the concept in order to assess whether the technology or technical devices used in iBorderCtrl or in smart border scenarios in general, constitute a case of unequal treatment (i.e. if certain groups or individual group members are treated differently, in comparison to similar groups or similar individuals).

If a case of unequal treatment is established, this does not mean that automatically every case of unequal treatment constitutes a violation of human rights and is therefore rendered illegal. But in a second step, it needs to be established, whether such action or omission occurs without justification or factual reason.

#### 4.2.2.1 Legal sources of non-discrimination and equality

As a starting point it may be mentioned that from the various legal sources pertaining to the concept of equality there are three categories of legal sources, which are particularly relevant for the concept of equality and non-discrimination in Europe. EC law and European human rights law as well as the constitutional traditions of the European Member States.

The Charter of Fundamental Rights of the European Union (CFREU, 2000/C 364/01), deals with equality in chapter III, i.e. Art. 20-26. Of particular importance are Art. 20 (Equality before the law: Everyone is equal before the law) and Art. 21 (Non-discrimination) which reads:

*1. Any 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 shall be prohibited.*

*2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.*

Similar to the CFREU the European Convention on Human Rights (ECHR) prohibits discrimination in Art. 14 (“*The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.*”)

On top of this constitutional and legal traditions of the member states must be considered. Almost all EU / EEA Members States do have constitutional provisions concerning equality and/or discrimination. For example Art. 3 (Equality before the law) of the German Basic Law reads:

*(1) All persons shall be equal before the law.*

*(2) Men and women shall have equal rights. The state shall promote the actual implementation of equal rights for women and men and take steps to eliminate disadvantages that now exist.*

*(3) No person shall be favoured or disfavoured because of sex, parentage, race, language, homeland and origin, faith, or religious or political opinions. No person shall be disfavoured because of disability.*

From the cited above, it may not be assumed that discrimination, particularly on the grounds mentioned is in any case illegal, but rather that a legal justification is required for any discriminatory measure. Similar to the concept of proportionality in data protection, one may argue that, in order to assess the proportionality of a legislative measure discriminating a certain groups, the rationale of such measures must be tested against the possible violation of such groups or individual group member's human/fundamental rights. The more an individual is affected in his/her fundamental rights, the more such individual may be unable to avoid or circumnavigate a situation in which his/her fundamental rights may be violated, the higher or stricter are the requirements as to the legal justification of a measure that may be regarded discriminatory.

The legal concept of proportionality is (beyond data protection) well established and recognised as one of the general principles of European Union law.<sup>9</sup> It is also recognised in Article 5 of the EC Treaty, stating that "any action by the Community shall not go beyond what is necessary to achieve the objectives of this Treaty".

Proportionality of a measure could be established by means of a three-step test. Firstly, "suitability" of a measure must be ascertained. Suitability test defines whether a measure (involving discrimination of certain groups or individuals) is reasonably likely to achieve its objectives. Secondly, "necessity" of a measure must be tested. The necessity test evaluates whether there are other less restrictive means capable of producing the same result. Thirdly, "proportionality" *strictu sensu* must be established. This means that the scale of discrimination is weighed against the importance of the objectives pursued. Regarding the last step of the three-step-test it must be emphasised, that from an ethical point of view, it would be more difficult to justify a discriminatory measures based on sex, race, colour, language, religion, political or other opinion, national or social origin and association with a national minority, property or birth.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

<sup>9</sup> See *Federation Charbonniere de Belgique v High Authority* [1954] ECR 245 Case C8/55[11]; *Internationale Handelsgesellschaft v Einfuhr- und Vorratsstelle Getreide* [1970] ECR 1125 Case 11/70; *R v Minister of Agriculture, Fisheries and Food ex parte Fedesa* [1990] ECR I-4023 Case C-331/88



## **4.3 Human Dignity**

### **4.3.1 Legal Background**

#### **4.3.1.1 Introduction**

Human dignity describes the concept of an individual's or group's right to be valued and respected. The concept may by many people be understood intuitively and, very generally, expresses the requirement of fair and ethical treatment of every human being who shall be endowed with inherent and inalienable rights.

From an ethical perspective individual's or group's dignity may be violated in multiple ways. Aside from the most obvious examples of a violation of human dignity such as torture, slavery, bonded labour or putting human beings into inhuman living conditions, there may also be cases where an interference with human dignity is less obvious and where a violation of human dignity may have numerous facets and dimensions. For example to humiliate i.e. embarrass a person and subject them to public ridicule. Furthermore, a person may be "dehumanized" that refers to an act with which individuals or groups are stripped of their human characteristics or treated as less valued human beings. Human dignity may also be violated by degradation, where the inherent value of a human being is deprecated. This even may be a violation of human dignity if it is done with consent, which at first sight seems like an autonomous decision, but in reality is an act with which an individual effectively "surrenders" his/her autonomy and human dignity. Furthermore, and of particular emphasis within iBorderCtrl, shall be the dimension of instrumentalization an objectification. Objectification means to reduce a human being to an object or thing for example in order to use someone to reach other goals, to treat someone as if he/she does not possess physical or psychological boundaries, to treat someone with no concern for their feelings and individual experiences. Furthermore, autonomy and self-determination shall be mentioned in this context and an act which displays a lack of respect for a person's autonomy may be seen as a violation of human dignity as well.

#### **4.3.1.2 Legal Sources of Human Dignity**

The different facets of human dignity that have been briefly mentioned above, pose certain challenges and difficulties for a legal interpretation and approach to human dignity. As a legal concept human dignity is hard to describe and it may safely be argued that the concept does not provide a universal and well established basis for judicial decision-making and judicial review. In a legal sense there probably is little common understanding of what dignity requires substantively within a certain jurisdiction or even more difficult across jurisdictions in international public law and human rights context. The value and meaning of human dignity rather depends on the context in which it occurs and may vary significantly among different jurisdictions and "instead of providing a basis for principled decision-making, dignity seems open to significant judicial manipulation, increasing rather than decreasing judicial discretion."<sup>10</sup> Despite the numerous dimensions and differences regarding the interpretation of all the facets of the concept it must not be omitted that the term human dignity has of course made its mark in various international treaties, constitutions and other legal texts and judgments.

---

<sup>10</sup> Christopher McCrudden, Human Dignity and Judicial Interpretation of Human Rights, EJIL (2008), Vol. 19 No. 4 , 655 – 724, 655.

Most prominently and a source of inspiration for subsequent legal text emanates from the use of dignity in the Universal Declaration of Human Rights (UDHR). The Preamble already mentions dignity on two occasions and: “whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world ...” and: “whereas the peoples of the United Nations have in the Charter reaffirmed their faith in fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women and have determined to promote social progress and better standards of life in larger freedoms”. Art. 1 reads: “all human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.” Moreover, there are several further occasions where the term dignity is used in the UDHR.<sup>11</sup>

The concept of dignity is not restricted to the sphere of international human rights law, but has subsequently been included into regional human rights instruments.<sup>12</sup> Although it was not included in the text of the European Convention on Human Rights (ECHR), it has been picked up in several later Council of Europe conventions, e.g. notably the Revised European Social Charter<sup>13</sup> and the Convention on Human Rights and Biomedicine.<sup>14</sup>

For the territory of the European Union the concept of human dignity is reinforced by the EU's charter of fundamental rights (CFREU) which provides in its Preamble: “Conscious of its spiritual and moral heritage, the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity”. CFREU makes the protection of dignity an explicit commitment and provides in Art. 1: “Human dignity is inviolable. It must be respected and protected.” It goes on with Art. 2 (Right to life), Art. 3 (Right to the integrity of the person), Art. 4 (Prohibition of torture and inhuman or degrading treatment or punishment) and Art. 5 (Prohibition of slavery and forced labour) which may be viewed as further manifestations and facets of the concept of human dignity.

The concept of human dignity has furthermore been incorporated into national constitutions. In particular, the German constitution and its interpretation by the German Constitutional Court was a strongly influenced subsequent national European constitutions, especially after the fall of the so called “iron curtain”.<sup>15</sup> Art 1(1) of the German Basic Law (Grundgesetz) reads: “Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority.” Furthermore, it must be mentioned that the concept of human dignity has been subject to judicial interpretation in various cases brought before the German Constitutional Court (Bundesverfassungsgericht). In a judgment delivered in 2006, the Constitutional Court had to weigh the concept of human dignity against a law which proposed the shooting-down of any unidentified aircraft that, carrying hostages, might pose an imminent threat to certain important ground structures and/or a large number of civilians. The

---

<sup>11</sup> e.g. Art. 22 reads: everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality”; Art. 23(3) reads: “everyone who works has the right to just and favourable remuneration ensuring for himself and his family an existence worthy of human dignity, and supplemented, if necessary, by other means of social protection”.

<sup>12</sup> Pls. see Christopher McCrudden, Human Dignity and Judicial Interpretation of Human Rights, EJIL (2008), Vol. 19 No. 4, 655 – 724, 671.

<sup>13</sup> European Social Charter, ETS No. 163 (1996), Preamble, Art. 26.

<sup>14</sup> Convention on Human Rights and Biomedicine, CETS No. 164 (1997), Preamble, Art. 1.

<sup>15</sup> Pls. see Christopher McCrudden, Human Dignity and Judicial Interpretation of Human Rights, EJIL (2008), Vol. 19 No. 4, 655 – 724, 673.

Constitutional Court held the law unconstitutional arguing that the decision to shoot down an unidentified aircraft and thereby sacrificing hostages on board of the aircraft may compromise human dignity. In particular the court held: "The duty to respect and protect human dignity generally forbids making any human being a mere object of the actions of a state. Any treatment of a human being by the state that - because it lacks the respect for the value that is inherent in every human being - would call into question his or her quality as a subject, his or her status as a subject of law, is strictly forbidden."<sup>16</sup>

## **4.4 Risk of Stigmatization and the Impact of Technology**

### **4.4.1 Definition and Classification of False Positives & False Negatives in the Legal Framework**

[REDACTED]

<sup>16</sup> BVerfG, Urteil des Ersten Senats vom 15. Februar 2006 - 1 BvR 357/05 - Rn. (1-156), Rn. 121.

[REDACTED]

#### 4.4.2 Ethical implications of false positives

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### 4.4.3 Impact on the Individual vs. Impact on Other Travellers

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

<sup>17</sup> See, Handbook for Schengen Border Guards, p. 57 f., available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015010%202006%20INIT.p 57>.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

#### **4.4.4 Data Quality and Falsified Information**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 4.5 Profiling of travellers

‘Profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.<sup>18</sup> [REDACTED]

[REDACTED] From a legal point of view, profiling poses a variety of risks: Due to the nature of profiling, the collection of different kinds of personal data is required. While the collection of personal data in itself is already subject to certain restrictions (requires a legal basis

---

<sup>18</sup> See Article (4) (4) of Regulation 679/2016/EU and Article (3) (4) of Directive 680/2016/EU. Please also see 4.6

or consent of the data subject), the concentration of different categories of data of a person in the hands of one data controller may cause a severe intrusion into the privacy of a data subject. Profiling, therefore, is subject to specific legislation: According to Article 22 of the GDPR, data subjects may have the right to not be subject to profiling that results in legal effects concerning the data subject or similarly significantly affects him or her. Article 11 of Directive 680/2016/EU prohibits profiling in general, unless appropriate safeguards are applied. The increased risk that arises from profiling therefore is inherited in the legal system and therefore needs specific attention in iBorderCtrl as well.

[REDACTED]. As outlined above, it is important to ensure that these risk indicators do not discriminate against certain groups of persons without proper justification, in order to mitigate risks of stigmatisation and thus preserve traveller's human dignity and right to equal treatment.

#### 4.5.1 Proposed Risk Indicators

[REDACTED]

	[REDACTED]	[REDACTED]
■	[REDACTED]	[REDACTED]
■	[REDACTED]	[REDACTED]
■	[REDACTED]	[REDACTED]
■	[REDACTED]	[REDACTED]
■	[REDACTED]	[REDACTED]



■		
■		

[REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

#### 4.5.2 Proposed risk thresholds

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[illegible]

## 4.6 Automated Decision Making

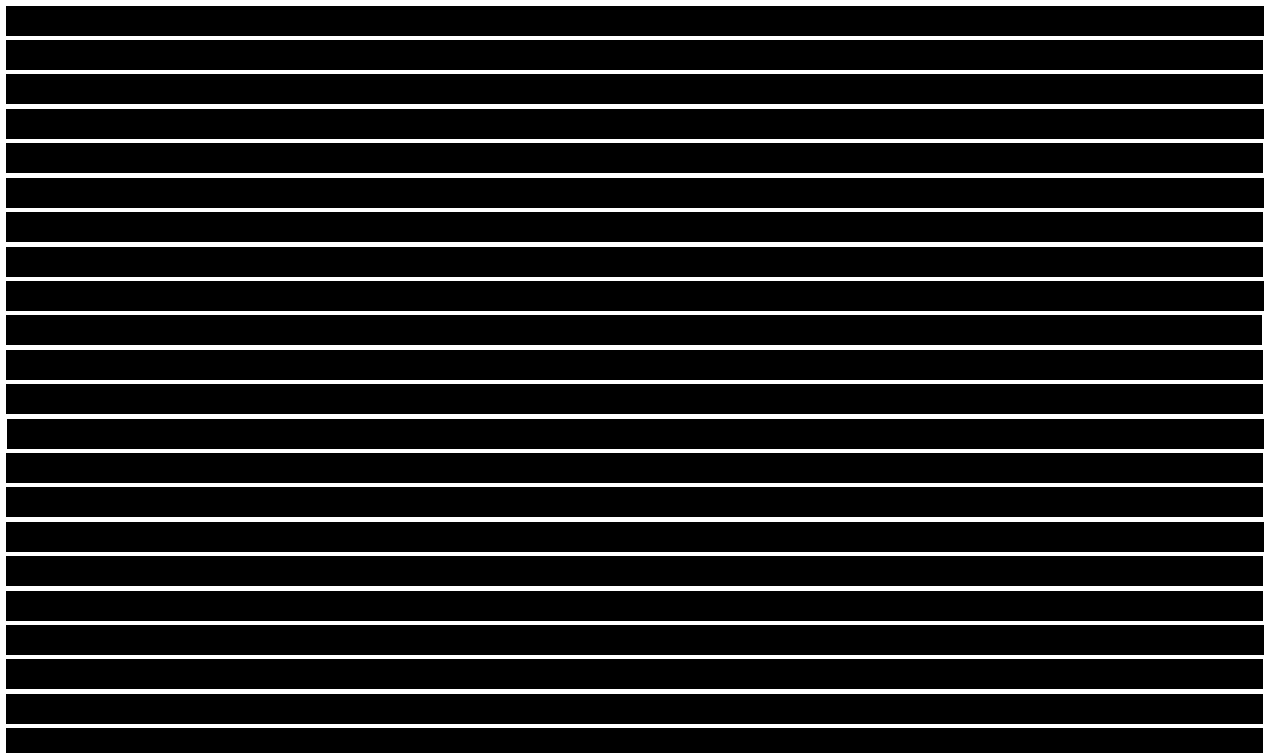
[illegible]

The basis of legal / ethical considerations regarding automated decision making processes in the context of iBorderCtrl is again - like in the case of profiling - Art. 11 Directive 680/2016/EU. Article 11 of Directive 680/2016/EU prohibits decisions based solely on automated processing, unless appropriate safeguards are applied.<sup>22</sup>

22 Art. 11 (1) Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller.

From a legal point of view it must be re-emphasised that Directive 680/2016/EU as well as Directive 679/2016/EU (GDPR) mentioned “profiling” and “automated decision making” together. However, and despite both terms overlap to a great extent, they are two separate things.

Whereas profiling means broadly speaking, “gathering information about an individual or group of individuals and analysing their characteristics or behaviour patterns in order to place them into a certain category or group, and/or to make predictions or assessments about *inter alia* ability to carry out a certain task or individual interests and/or preferences.”<sup>23</sup> In contrast to this, automated decision making, refers to the ability to make decisions based on certain information including personal information such as profiles without human interaction. The difference can be seen in the fact that automated decision making is the process of coming to a decision based on an already created profile. That means a collection of data is used to create a profile upon which then an automated decision can be made; can, however, also be taken by a human.<sup>24</sup>



---

(2) Decisions referred to in paragraph 1 of this Article shall not be based on special categories of personal data referred to in Article 10, unless suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(3) Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law.

<sup>23</sup> Information Commissioner's Office, Feedback request – profiling and automated decision-making, 06.04.2017, P. 5 et seq. <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf> last accessed on

<sup>24</sup> Andrej Savin, Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks, P. 1. <http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf?sequence=1> last accessed on



## **4.7 Impact of Human-Machine Interaction**

The interaction between humans and machines is an integral part of the ADDS system and the avatar interview. The purpose of those functionalities is to shift certain elements of the border check from the border crossing phase to the pre-registration, and, in consequence, from an interaction between border guards and travellers - both as human beings - to an interaction with a computer avatar. Neither the use of such technology nor guidelines regarding the interaction of humans and machines with regard to border checks are incorporated in the current legal system.

According to Article 7 SBC, border guards shall, in the performance of their duties, fully respect human dignity, in particular in cases involving vulnerable persons. This might even more apply if certain aspects of the border check are not being performed by border guards, but by an avatar. Additionally, Article 16 SBC stipulates that Member States shall ensure that the border guards are specialised and properly trained professionals, taking into account common core curricula for border guards. These training curricula shall include specialised training for detecting and dealing with situations involving vulnerable persons, such as unaccompanied minors and victims of trafficking. These requirements very much reflect the concerns that arise when performing border checks: Both the behaviour of border guards as well as the measures performed during a border check have to fully respect human dignity. To this extent, the importance of decisions such as access or refusal as well as the intensity of checks on the privacy have to be considered as well. With regard to the avatar interview, a variety of issues arise:

### **4.7.1 Degradation of the Traveller to an Object**

By having an interview with a computer avatar instead of a border guard, the traveller will be faced with a rather unusual environment: In fact, an interaction between humans and machines cannot be found in any other area of daily life either. While there are certain approaches to facilitate the use of ICT-technology in certain areas, such as the consultation of a medical doctor via a webcam, there is still a human being actively involved.

In order to fully understand the implication that arises from replacing human interaction with machine interaction, it is important to show the actual difference. Computer software usually follows a set of rules, specifying how the software should behave in certain situations. However, it is not possible to properly assess every detail in every situation. Therefore, computer software is not able to adapt to a situation in the same way a border guard could. If, for instance, a person feels bad or starts crying, how could software adapt to this situation? Even if the avatar would be able to detect such behaviour, it would not be able to actually help the person by calming him/her down.

In addition, due to the technical nature of the avatar, a conversation would have to follow certain rules. In order to allow the software to properly process the answers, questions have to be asked in a specific way in order to receive the answer in a specific format. The wording of those questions could appear to be strange to travellers. Another particular aspect caused by the technical nature of the avatar is that the avatar cannot react to certain circumstances. If a traveller, for instance, is not able to properly reply to a question, e.g. because there is a non-typical situation which is not covered by the questions/answers, this could cause further implications: On the one hand, travellers could feel

helpless due to the fact that the avatar cannot give them any feedback on their particular issue. On the other hand, such situations cannot be properly processed by the software and could lead to wrong decisions regarding the credibility of the traveller. As the avatar will also adjust its behaviour according to the behaviour of the traveller, wrong interpretations of the software could cause the avatar to react in a way which appears to be strange or frightening to the traveller.

It also has to be noted that the outcome of the avatar interview will be made available to the border guards at a border crossing point. While this means that certain aspects of the interview could be clarified with the border guards, it can be assumed that this will not only require additional efforts by the traveller, but also create a certain bias with regard to the border guards. Due to the fact that the time that a border guard spends with a traveller is reduced, there is also less time to develop an interpersonal relation with the traveller. This will increase the overall distance of the border guard with the traveller and therefore supplements the effect that a traveller could feel to be treated rather as an object than as a human being.

This obviously poses difficult ethical challenges with regard to human dignity. The avatar interview should therefore seek to implement safeguards which ensure that situations as outlined above cannot occur. To this extent, it needs to be further elaborated during the development of the avatar interview whether it is possible from a technical point of view to tackle those challenges.

This being said, the last aspect to be considered with regard to human-machine interaction is “time”. While the use of such technology is not common yet, it might be possible that human-machine interaction will be increasingly used also in other fields of daily life. Once people start to get used to the use of such technology and respective issues that may arise, the ethical assessment might change, as in this case the impact on travellers would be less intense.

#### **4.7.2 Cultural and Religious Implications**

Another important aspect is that the overall format of the avatar interview should not violate the cultural or religious feelings of travellers. In this regard, it has to be distinguished between the research and the exploitation phase:

[REDACTED]

#### **4.7.3 Questions asked during the Avatar Interview**

The questions raised during the avatar, from a legal point of view, have to be seen as data collection, as the answers of the traveller will be recorded and analysed. Following the principles stipulated in Article 8 ECHR, a statutory legal basis or consent of the traveller would be required in order to collect data. In order to allow a smooth implementation of iBorderCtrl in the current legal system, the questions raised should not differ from those that are currently being asked by border guards when performing border checks. This also ensures that the questions raised are being covered by a legal basis.



However, certain additional safeguards are required in order to ensure that no violations of ethical requirements can occur. [REDACTED]

[REDACTED]

#### 4.8 Function Creep

Another (also) ethical issue that needs to be observed within the context of iBorderCtrl is the problem of “function creep”. The European Commission describes function creep as “technology and processes introduced for one purpose [and] extended to other purposes which were not discussed or agreed upon at their implementation”.<sup>25</sup>

This means, when personal data is being collected and used for one specific predefined and legitimate purpose in order to fulfil a specific function, function creep describes the phenomenon of a subsequent shift of purpose due to gradual technological development and changing technological possibilities. Something that was once considered a socially, ethically and legally acceptable purpose may be “creeping” or may have crept towards another purpose which, at a certain point, is beyond what was originally intended and understood.

While function creep is closely connected with the notion of privacy in general and the data protection principle of purpose limitation and, in the context of informed consent, with the principle of transparency, it should not be omitted that it also is an ethical issue for the legislator as well as governments to consider.

It has been a serious concern especially in the context of biometric technologies and surveillance systems. Since such information technology systems were first used, function creep may be a well-known and addressed risk, yet it needs to be reemphasised that the higher technical potential of new computer systems raises the risk of data being used against their original purpose.<sup>26</sup> And it can be said that the potential of re-purposing and, especially, data linkage, both by governments and private companies can be a major threat to privacy.<sup>27</sup>

For the iBorderCtrl as well as for a subsequent exploitation of the technologies and devices that have been developed during the projects lifespan, it is therefore vital to periodically review the systems used and technical advancements that have been made or implemented. Not only to raise ethical concerns and identify potential threats to privacy of travellers but also to assess whether the technology used is still operated within the original purpose for which the system has been set up or the purpose the legislator has defined.

---

<sup>25</sup> European Commission Directorate-General Joint Research Centre, Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Executive Summary, 2005, p 7

<sup>26</sup> Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP193, p.17.

<sup>27</sup> House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15, p.27.

## 5 Concept of Informed Consent

As it has been emphasised before, it is not only important to comply with legal requirements that have been raised in Deliverable 2.3, but also ethical standards (which necessarily overlap with legal requirements) need to be observed. One ethical aspect of particular importance is the doctrine of informed consent. For the iBorderCtrl the concept of informed consent bears two implications. From an ethical point of view it may be viewed a matter of common decency and a token of respect that we owe to persons, trial participants, traveller and data subjects and provide a reason or justification for obtaining the travellers consent. A certain level of transparency in a border crossing scenario can also not be ruled out with a simple reference to public security and public safety and governmental organisations/agency must be held accountable in such areas as well. With regard to the principle of informed consent, transparency further aims to achieve the protection of the data subject's fundamental rights to autonomy and self-determination when her/his data are being processed. Every traveller is a human being after all and should therefore not simply be used as a means or degraded to an object of governmental manipulation. Instead, one should act in accordance with traveller's wishes and respect his/ her autonomy.

For the research phase as such the very core of this doctrine is the principle that any scientific research involving the collection and use of personal information can only be achieved by accepting a free and informed consent, prior to the collection of data. Moreover, consent should be explicitly expressed and the participant shall have the right to withdraw his or her consent at any time and for any reason without any disadvantages.

For a possible exploitation phase, from an ethical point of view, it should firstly be discussed to what extent it is / should be admissible to rely on informed consent in the first place. As far as consent is admissible under an amended legal framework, because inter alia iBorderCtrl technologies create an entirely separate, additional and voluntary means of crossing the border, it is vital to ensure that free and informed consent was given by the data subject, before collection of data commences.

The distinction between both phases which is being reflected in the legal assessment has to be considered for ethical issues as well in order to incorporate the different valuation standards that are subject to the different the legal frameworks. In fact, the circumstances under which a person is requested to give his/her valid consent is crucial for assessing whether this could cause ethical issues. General guidelines how a person should be treated in order to obtain informed consent in a lawful way are outlined in the recitals of the GDPR. Hence, the following sub-sections will incorporate these general principles and ideas of the GDPR as a basis for the identification of ethical issues. However, it has to be noted that those principles have to be carefully evaluated against the different challenges posed by iBorderCtrl in order to ensure that the (fundamental) rights and freedoms of the data subject are not being violated.

### 5.1 General Principles

According to Article 8 (1) ECHR, everyone has the right to the protection of personal data concerning him or her. As stipulated in (2), such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. According to Article 4 (11) of the GDPR, 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In general, the principle of informed consent aims to achieve the protection of the data subject's fundamental rights to autonomy and (informational) self-determination for the collection and processing of personal data. A human being asked for informed consent must not be used merely as a means, for instance to enhance the effectiveness of border checks in order to save time and/or personnel cost. Instead, one should act in accordance with the traveller's wishes and respect his or her right of self-determination. Therefore, the following elements should be reflected in the informed consent procedure:

### **I. The consent must be voluntarily given and devoid of any coercion.**

At the core of the principle of informed consent stands the idea that any data processing with regard to border checks can only be achieved by accepting a prior, free and informed consent from the traveller. Consent should cover all processing activities carried out for a defined purpose. When the processing has multiple purposes, consent should be given for all of them. According to recital 33 of the GDPR, consent may be given to certain areas of research if it is not exactly clear yet for which purposes a data processing is happening. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.<sup>28</sup>

In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.<sup>29</sup> As far as iBorderCtrl is concerned, the data controller would be border guard authorities, which are – by their nature – public authorities. As far as the research phase is concerned, this is however not quite relevant, as data would be collected for research purposes only, meaning that executive powers of public authorities will not be relevant for the volunteers.

According to recital 43 of the GDPR, consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

With regard to the research phase, there are no ethical issues which could prevent iBorderCtrl from complying with those requirements.

However, following this distinction between research and exploitation phase, different legal frameworks – and therefore different valuation standards - would apply: In contrast to the GDPR, Directive 680/2016/EU does not contain any provision that would allow to base a measure on informed consent. This becomes clear when consulting recitals (35) and (37). Recital (35) states:

The performance of the tasks of preventing, investigating, detecting or prosecuting criminal offences institutionally conferred by law to the competent authorities allows them to require or order natural persons to comply with requests made. In such a case, the consent of the data subject, as defined in Regulation (EU) 2016/679, should not provide a legal ground for processing personal data by competent authorities. Where the data subject is required to comply with a legal obligation, the data subject has no genuine and free choice, so that the reaction of the data subject could not be considered to be a freely given indication of his or

---

<sup>28</sup> Ibid.

<sup>29</sup> Regulation 679/2016, recital 43.

her wishes. This should not preclude Member States from providing, by law that the data subject may agree to the processing of his or her personal data for the purposes of this Directive, such as DNA tests in criminal investigations or the monitoring of his or her location with electronic tags for the execution of criminal penalties.

In recital (37), consent as a legal basis, again, is explicitly ruled out: “However, the consent of the data subject should not provide in itself a legal ground for processing such sensitive personal data by competent authorities.”

However, according to recital 35, the exclusion of consent as a legal basis for data processing under Directive 2016/680/EU does not preclude the Member States from providing by law that data subjects can agree to the processing. In that case, this agreement is not the legal basis for processing – which instead needs to be laid down in a law – but only an additional safeguard, granting the data subjects more rights and therefore increasing proportionality of the data processing [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## **II. Necessary information has been supplied to the subject of the consent to enable him or she make an informed decision as to whether to consent or not.**

In order to allow a person to give his informed consent, a fundamental requirement is that the data processing has to be made as transparent as possible to the data subject. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended.<sup>30</sup> [REDACTED]

<sup>30</sup> Regulation 679/2016, recital 42.

– however, information about the fact that and which data is being processed, as well as the respective purposes, should be provided as minimum requirement.

**III. There should be an opportunity for the consent giver to revoke this consent without suffering any harm as a result of the revocation.**

As described above, a traveller can only provide his/her informed consent only on the basis of a free decision. Vice versa, there is usually no statutory legal basis for the data processing, as in such cases, obtaining informed consent would not be necessary. In order to respect the doctrine of self-determination, a data subject must have the opportunity to revoke his/her consent any time. As both processes – declaring and revoking informed consent – have to be based on a free decision, it has to be ensured that no negative consequences arise for the data subject. This requirement includes both “legal” consequences such as a refusal at the border crossing point, as well as any other harm, such as additional checks or waiting times. To this extent, one possible risk that could arise is a stigmatisation based on the decision of a traveller: Without prior sensitisation and training, border guards could assume that persons who revoke their consent would have something to hide, therefore assuming that their behaviour is suspicious. The legal framework, allows border guards to perform thorough checks if they have a justified suspicion. While revocation of consent itself cannot be seen as a justified reason for further checks, border guards could tend to unconsciously be stricter with their controls compared to other travellers. Consequently, border guards should be aware of the fact that travellers have a right to self-determination and that the revocation of consent is a behaviour which must not be seen as suspicious, but as the enforcement of fundamental rights.

In addition to the revocation of consent, a data subject should have the right to have his or her personal data erased and no longer processed.<sup>32</sup>

**IV. The giver of the consent must have the legal competence to do so (such as not being a minor or not mentally capable of giving such consent).**

A further requirement for the validity of the consent is that the data subject is mentally capable to take decisions. Obtaining informed consent from minors and disabled persons can be subject to certain restrictions, as those groups require particularly high safeguards. To this extent, data protection law distinguishes between three groups of people:

- I. This is no problem when persons concerned have attained legal age and are contractually capable.
- II. If a person is a teenager, but not of legal age yet, obtaining informed consent might be possible under certain restrictions.
- III. In other cases, where the data subject is mentally incompetent and/or a minor, informed consent has to be requested from the legally authorised representative.

Following this distinction, particular ethical issues arise for group II. According to recital 38 of the GDPR, Children merit specific protection with regard to their personal data, as they may be less aware

<sup>31</sup> This will be further elaborated when developing the test pilot methodology as outlined in Task 6.1.

<sup>32</sup> See recital 65 of the GDPR.

of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. However, according to article 8 (1) GDPR, the processing of the personal data of a child in relation to the offer of information society services directly to a child shall be lawful where the child is at least 16 years old. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years. According to article 4 (25) GDPR, ‘information society service’ means a service as defined in point (b) of Article 1 (1) of Directive (EU) 2015/1535 of the European Parliament and of the Council, which means “any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.”

As outlined above, certain exemptions may apply to teenagers. However, it has to be noted that minors (and disabled persons) will not be subject to the research phase of iBorderCtrl. For the exploitation phase, the GDPR will not apply, though. At the same time, “*children and fools always speak the truth*”<sup>33</sup> – making them particularly vulnerable to data processing in the field of public security. With regard to border crossing, there are specific rules for minors.<sup>34</sup> In addition, border guards shall be specialised and properly trained, including a specialised training for detecting and dealing with situations involving vulnerable persons, such as unaccompanied minors.<sup>35</sup> In this regard, there is no distinction between minors and minors in the age of 13 – 18 years. Apart from the overall treating of minors as outlined above, minors crossing an external border shall be subject to the same checks on entry and exit as adults as outlined in the SBC.<sup>36</sup>

However, it has to be noted that the SBC itself does not contain any voluntary checks and measures. Consequently, situations in which minors would have to decide on their own whether they would like to agree to a certain measure are not covered by the SBC. From an ethical point of view, minors in the age between 13 and 18 years require additional protection as well: Border guard authorities, which are often part of the police authorities, have extensive executive powers – legal consequences therefore might not be restricted to a thorough check or a refusal at the border crossing point, but could also potentially lead to arrest in case that a criminal offence has been revealed. These consequences are not comparable to a consent as referred to in Article 8 GDPR: While the legal consequences arising from a data processing within the scope of the GDPR would only affect informational self-determination and the right to privacy, legal consequences deriving within the scope of iBorderCtrl could affect the fundamental right to freedom or property as well. Considering this potentially intense impact, the safeguards for such a measure have to be designed respectively.

Further ethical issues regarding minors might arise regarding the requirement that vulnerable persons – such as minors – should be treated by specialised and trained border guards. Certain functionalities such as the avatar interview might not be able to react to the specific needs of minors, and therefore to meet these high standards as outlined in the SBC.<sup>37</sup> Consequently, the iBorderCtrl system should not offer minors the possibility to consent into such measures at all.

All in all, allowing persons of group II. the possibility to consent into the use of iBorderCtrl should be avoided in order to ensure high ethical standards. Therefore, consent should be requested from

<sup>33</sup> Mark Twain, On the Decay of the Art of Lying, available at <http://www.gutenberg.org/cache/epub/2572/pg2572-images.html>.

<sup>34</sup> See Article 20 (1) (f) SBC.

<sup>35</sup> See Article 16 (1) SBC.

<sup>36</sup> Annex VII number 6.1 SBC.

<sup>37</sup> See section 4.2.3..

persons which are of legal age and mentally capable, while consent should be requested from legally authorised representatives if a person is a minor or mentally incompetent.

## **V. Other formal requirements**

Other formal requirement must be observed where they exist. A particularly relevant requirement in this regard could be to ask travellers for their written consent. According to recital 32 of the GDPR, consent might be given by a written statement, including by electronic means, or an oral statement.

[REDACTED]

## **5.2 Ethical issues regarding the effectiveness of measures based on informed consent**

As outlined above, consent is not to be seen as a “usual concept” for data processing in the field of law enforcement. Therefore, applying consent in the field of public security requires specific attention, in particular from an ethical point of view. A fundamental principle of the doctrine of informed consent is that travellers would provide border guard authorities with information on a voluntary basis. On the contrary, travellers would also have the right to not provide this information to border guard authorities.

However, in order to ensure the effectiveness of border checks – which have an immediate impact on public security – every traveller has to undergo an appropriate check. Persons who are not eligible for entering the Schengen area would in such cases most probably avoid any voluntary measures, as this could – from their point of view - increase the risk of a refusal.

[REDACTED]

---

<sup>38</sup> According to recital 42 of the GDPR, where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In accordance with Council Directive 93/13/EEC (1) a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.



Apart from the issue of stigmatisation, further ethical issues might arise from the fact that the effectiveness of border checks will change if different processes apply to travellers depending on their consent. Naturally, border checks performed by human beings only will lead to different results compared to border checks performed with the support of IT-systems.<sup>39</sup> This could, however, exceed the scope of Article 8 (1) ECHR, as data subjects shall only decide about whether their personal data is processed, not about a possible effect on public security. This being said, it has to be noted that the Member States are responsible for ensuring and maintaining public security. Consequently, measures that involve the processing of personal data – such as certain measures used during border checks – should be mandatory (and effective), or, if this is not the case, they should not be applied at all. This being said, citizens should not be able to consent to data processing if this decision could have an immediate impact on public security. Neither should citizens be – in any way – responsible for maintaining public security, nor should the degree of public security depend on the voluntary participation of citizens. In this regard, it has to be noted that certain fundamental rights, such as the right to life and physical integrity, require Member States to enforce public security, also by limiting other fundamental rights, such as the right to privacy, to a certain extent. In general, measures that require the processing of personal data in the field of public security should not be based on consent, if possible. Regardless of whether iBorderCtrl or the standard procedure work more efficient, Member States would have to explain citizens why they – either way – apply less effective measures to a certain group of travellers, therefore posing a risk to public security.

However, there might be certain exemptions from these general thoughts. If it can be ensured that the result of a measure is exactly the same both by using iBorderCtrl and conventional tools, consenting into measures could be possible, as there would be no (potentially) negative impact on public security. This would be, for instance, the case for a biometric identification. Assuming that both procedures work effectively, a person might consent into using palm vein recognition instead of fingerprints to uniquely identify him or her without affecting public security at all.

---

<sup>39</sup> For further details, see section 4.



## 6 Risk Mitigation Plan

According to the DoW, the ethics of profiling and the risk of stigmatization of individuals and groups must be addressed in the context of WP2 and linked to the possibility of false positives. Furthermore, an appropriate mitigation plan must be included in D2.2 (Reference Architecture and Components Specifications). Following the Ethics Summary Report, the aim of the ethics deliverables is to minimise any negative impacts on volunteers participating in iBorderCtrl. The risk mitigation plan will, however, also cover the exploitation phase and provide general recommendations on how certain risks with regard to ethical issues could be avoided. As the legal framework to be applied during the research phase, for instance for the test pilots, differs from the legal framework to be applied for a (commercial) exploitation and a usage in real border-check scenarios after the project end, the mitigation measures are listed according to every phase.<sup>40</sup>

### 6.1 Research Phase

#### 6.1.1 Overall Design of the Test Pilots

[REDACTED]

[REDACTED]

[REDACTED]

#### 6.1.2 System requirements

[REDACTED]

[REDACTED]

### 6.1.3 Anonymisation and Pseudonymisation

[REDACTED]

### 6.1.4 Transparency and Training

[REDACTED]

[REDACTED]

### 6.1.5 Legal obligations for all parties involved

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 6.2 Exploitation Phase

[REDACTED]

[REDACTED]

---

<sup>42</sup> This requirement is, among others, also part of the data protection rules for iBorderCtrl (Article 2 (1) (b)) that has been accepted by all consortium partners.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 7 Conclusions

In summary, the ethical as well as the legal assessment of iBorderCtrl, its devices and the technology used reveals a number of ethical issues and concerns. There is a risk of stigmatisation, which is inter alia associated with data accuracy and quality depending on the data sources used to calculate the risk scores. There is a risk of false positives and iBorderCtrl must implement appropriate redress mechanisms to ensure that for instance inaccurate data will be disregarded and not be further processed. Furthermore, there are ethical risk connected with the profiling of travellers. Of particular relevance for the right to human dignity and the impact on it, is brought to the fore by the issue of automated decision making. Furthermore, this deliverable has highlighted ethical concerns related to the impact of human machine interaction. Since iBorderCtrl relies on an avatar interview as a distinct item of the registration phase that, inter alia incorporates a technique of Non-verbal behaviour analysis (NVB). Further ethical concerns are raised by the issue of informed consent, since iBorderCtrl relies on consents as legal justification to process personal data, both during the research phase as well as afterwards in a possible exploitation scenario, it is a legal – ethical question to what extent one could rely on informed consent as a legal basis.

To conclude, it shall be highlighted that in order to mitigate the ethical risks for natural persons/travellers both in research phase as well as a subsequent exploitation phase, two decisive factors shall be emphasised in particular:

Firstly, thorough training and qualification of all persons involved in the use of iBorderCtrl components and devices shall be implemented. In particular border guards must be properly trained.

[REDACTED]

Secondly, and even more important, a system of an independent ethical oversight should be implemented. Although ethical review applies and is required in both stages (research and exploitation) it is suggested to implement a system of independent ethical approval and review, in particular in the exploitation phase, covering every ethical/legal aspect that is raised by iBorderCtrl and the technology used.

[REDACTED]

## 8 References

Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, WP193

BVerfGE 65, 1 - Volkszählung

BVerfG, Urteil des Ersten Senats vom 15. Februar 2006 - 1 BvR 357/05 - Rn. (1-156), Rn. 121

European Commission Directorate-General Joint Research Centre, Biometrics at the Frontiers: Assessing the Impact on Society. For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Executive Summary, 2005

Federation Charbonniere de Belgique v High Authority [1954] ECR 245 Case C8/55

Handbook for Schengen Border Guards, p. 57 f., available at <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2015010%202006%20INIT.p> 57

Hippocrates of Cos, "The Oath". Loeb Classical Library (1923) 147: 298–299. doi:10.4159/DLCL.hippocrates\_cos-oath.1923

House of Commons Science and Technology Committee, Current and future uses of biometric data and technologies, Sixth Report of Session 2014–15

[https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication\\_eas\\_progress\\_since\\_april\\_2015\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf)

[http://europa.eu/rapid/press-release\\_IP-17-1303\\_en.htm](http://europa.eu/rapid/press-release_IP-17-1303_en.htm)

Information Commissioner's Office, Feedback request – profiling and automated decision-making, 06.04.2017, P. 5 et seq. <https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf>

Internationale Handelsgesellschaft v Einfuhr- und Vorratsstelle Getreide [1970] ECR 1125 Case 11/70

McCrudden C, Human Dignity and Judicial Interpretation of Human Rights, EJIL (2008), Vol. 19 No. 4, 655 – 724, 655

R v Minister of Agriculture, Fisheries and Food ex parte Fedesa [1990] ECR 1–4023 Case C-331/88

Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5 (1890), pp. 193-220

Savin A, Profiling and Automated Decision Making in the Present and New EU Data Protection Frameworks, P. 1. <http://openarchive.cbs.dk/bitstream/handle/10398/8914/Savin.pdf?sequence=1>

Twain M, On the Decay of the Art of Lying, available at <http://www.gutenberg.org/cache/epub/2572/pg2572-images.html>