D3.1 Privacy, data protection, social & ethical issues preliminary guide

Document Due Date: M3
Document Submission Date: M3 (28/11/2019)

Work Package 3: Ethical, social and legal (including data protection and privacy) impact assessment

Document Dissemination Level: PU

D4FLY - **D**etecting **D**ocument frau**D** and i**D**entity on the fly
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833704

Abstract

This deliverable is a preliminary guide outlining key privacy, data protection, socio-cultural and ethical issues for the benefit of the partners gathering requirements for the D4FLY technologies in Task 2.2-system requirement analysis. It aims to help them understand some of the key issues required for ensuring that the technology is developed with a privacy by design approach. This deliverable is based on a desk-based literature review with specific attention to legal instruments including the GDPR and the ePrivacy Directive (and proposed regulation) as well as related standards, academic publications, and stakeholder insights. The aim of this guide is to provide an explanation of ethical and social issues such as autonomy, dignity, informed consent, trust, asymmetries of power, fairness, equity, and social categories (e.g., unintentional discrimination on the basis of age, gender, ethnicity, ICT proficiency and economic resources). It also examines material concerning similar ICT systems.

Project Information

Project Name	Detecting Document frauD and iDentity on the fly
Project Acronym	D4FLY
Project Coordinator	Veridos GmbH
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SU-SEC-2018
Topic	SU-BES02-2018-2019-2020 Technologies to enhance border and external security
Funding Instrument	Research and Innovation Action
Grant Agreement No.	833704

Document Information

Document reference	D3.1
Document Title	Privacy, data protection, social & ethical issues preliminary guide
Work Package reference	WP3
Delivery due date	30.11.19
Actual submission date	30.11.19
Dissemination Level	PU
Author(s)	Goldberg, Zachary; Muraszkiewicz, Julia
Contributor(s)	
Document Review Status	☐ Consortium ☒ WP leader ☐ Technical Manager ☐ Quality and Risk Manager ☐ Ethical Advisory Board ☐ Security Advisory Committee ☒ Project Coordinator

Document Version History

Version	Date created	Beneficiary	Comments
0.1	31.10.2019	TRI	Draft 1
0.2	05.11.2019	TRI	Review and edits by Julia Muraszkiewicz
0.3	08.11.2019	TRI	Draft 2
0.4	12.11.2019	VD	Review by Armin Reuter
0.5	13.11.2019	TRI	Draft 3
1.0	27.11.2019	VD	Final for submission

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
D	Deliverable
D4FLY	Detecting Document frauD and iDentity on the fly
EC	European Commission
EPIA	Ethics and Privacy Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
PIA	Privacy Impact Assessment
WP	Work Package

Table of Contents

1 INTRODUCTION 6
1.1 AIM OF THIS DOCUMENT FEHLER! TEXTMARKE NICHT DEFINIERT.
1.2 INPUT / OUTPUT TO THIS DOCUMENT 7

2 PRIVACY 8
2.1 SOME ISSUES PARTNERS SHOULD CONSIDER 8
2.2 The GDPR 9

3 ETHICS 11
3.1. SOME ISSUES PARTNERS SHOULD CONSIDER 11
3.2 ETHICAL OPPORTUNITIES 12
3.3 ETHICAL CONCEPTS 12
3.4 WHY ARE THESE CONCEPTS IMPORTANT? EXAMPLES. 14

4 COMPLIANCE WITH LAWS, REGULATIONS, CODES AND GUIDELINES 15

5 CONCLUSIONS 17

REFERENCES 18

LIST OF TABLES 19

ANNEX A 20

1 INTRODUCTION

This document has been produced by Trilateral Research, a partner in the consortium, for the D4FLY technical partners. It provides an introduction to some of the ethical and privacy parameters that may be taken into account as the consortium develops its technical solutions in a privacy by design manner. Privacy by design encourages a proactive approach of including privacy considerations at the outset rather than waiting for risk to materialise. As a result of the importance of privacy by design, Privacy Impact Assessments (PIAs) have gained in popularity over the last few years and it is now deemed to be best practice by many for technology developers, policy-makers, project managers to undertake a PIA throughout the design stage of a technological system. For the purpose of the D4FLY project, we include an ethical and privacy impact assessment (EPIA), which is a systematic process for identifying and addressing ethical and privacy issues in an information system, whilst also considering the future consequences and impacts of proposed actions in relation to ethics and privacy. The first step in this process is the current document, which provides an overview of ethical and privacy concepts relevant to D4FLY partners. By having access to the document partners who may not use privacy and ethical terms and concepts on a day-to-day basis can quickly and efficiently familiarise themselves with the same, thus also encouraging a better co-creational work flow. In summary, an EPIA is beneficial as it:

- Benefits to organisations, society and the individual (translate into wider economic and socio-economic benefits)
- Can reduce the risk of harm (privacy, ethical) to individuals
- Ensures that privacy/ethics are a key consideration in the life cycle of projects and programmes
- Ensures that research projects (e.g. H2020) include considerations of privacy/ethics in the development of new technologies and new technological systems
- Helps organisations maintain their reputation and mitigate reputational damage
- Helps organisations meet their legal requirements (e.g. data protection)
- Can help organisations in relation to their overall risk management strategy
- Can provide economic opportunities and benefits for organisations in relation to technological innovation and development
- PIAs become mandatory under GDPR
- GDPR (General Data Protection Regulation) – intention is to strengthen and unify data protection across the EU

The key question of an EPIA is:

Does my design enable ethical actions?

1.1 Aim of this document

Under a Trilateral approach, an EPIA incorporates a systematic process to mapping information flows, mapping and assessing risks, and providing a set of possible solutions for technology developers to take into account during the design stage of a system. An EPIA is proactive; it enables ethical and privacy-oriented solutions to be designed into the D4FLY technologies during development stage. Currently there is no agreed international standard

for an EPIA process. TRILATERAL will develop a **qualitative** EPIA methodology and framework that is most suitable to D4FLY. It will involve (as preliminary methodology as of today):

I. Developing an understanding of the D4FLY technology
II. Reviewing relevant literature, policy documents and legislation
III. Mapping the information flows: this describes and maps the flows of personal information in the D4FLY systems.
IV. Identify key ethical and privacy risks.
V. Identify key stakeholders.
VI. Initiate stakeholder consultation to evaluate:
- An ethical impact analysis: this identifies an analysis how the project impacts upon ethics
- A privacy impact analysis: this identifies an analysis how the project impacts upon privacy
- How to mitigate risks

VII. Consolidate all information and analyse the same to produce recommendations.
VIII. Recommendations: this produces a final EPIA report.

1.2 Input / Output to this document

Input is the research and literature review done by the author of the deliverable as well as knowledge acquisition of the technologies under development by D4FLY partners. Output is this deliverable.

2 PRIVACY

Privacy is a complex notion and in D4FLY we will rely on an approach that encompasses seven types of privacy:

i. **Privacy of the person** is defined as the right to keep body functions and body characteristics private.
ii. **Privacy of behaviour and action** refers to the ability of the individual to behave and do as she likes without being monitored.
iii. **Privacy of communication** relates to interception of communications such as recording and access to e-mail messages.
iv. **Privacy of data and image** involves the right of the individual to exercise control over personal data, rather than such data being available to organisations and others by default.
v. **Privacy of thoughts and feelings** refers to the individual's right not to share his or her thoughts and feelings or not to have these revealed.
vi. **Privacy of location and space** encompasses the right of the individual to freely move about in public, or semi-public space, without being monitored or tracked.
vii. **Privacy of association** refers to the right of the individual to associate with others without being monitored.[1]

It is also important to note that within the context of D4FLY privacy is a lot about personal data, which in turn is:

Personal data is any information relating to an identified or identifiable natural person. This is a wide and inclusive definition. There are also some categories of sensitive personal data (such as racial or ethnic origin, political or religious beliefs, health data) that get extra protection because abuse of personal data in these categories is likely to lead to harmful consequences. Processing of personal data is any activity performed on personal data (such as collecting, storing or organising it).

2.1 Some of the issues partners should consider include:

I. Data should be collected lawfully. This can be done through (see GDPR[2] Art. 6):

- The individual whom the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).

[1] Kroener, Inga, and David Wright (2015). "Privacy Impact Assessment Policy Issues" in Artemi Rallo Lombarte and Rosario Garcia Mahamut (eds.) Hacia Un Nuevo Derecho Europeo De Protección De Datos. Towards A New European Data Protection Regime, Tirant lo Blanch, Valencia.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation), but most often shorted to "the GDPR"

- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

II. Only the minimum amount of data should be collected.
III. Data should be stored securely. Information, which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a security risk.
IV. Data collected should only be retained for a proportionate and specified amount of time.
V. Collected data should be accurate, complete and up to date.
VI. The data subject should be aware as to what data is being collected and for what purpose. Partners should take steps to ensure that individuals can contact the organization for assistance if necessary.
VII. Data should not be disclosed, made available or otherwise used for purposes other than those specified except with the consent of the data subject or by the authority of law.
VIII. The data subject should have free access to data.
IX. The anonymity of the data subject should be protected.
X. Less privacy-intrusive alternatives should be considered.
XI. How the technology will affect 3rd parties who may not be able to consent to the technology needs to be considered.
XII. We have to ask who will authorize surveillance in public areas.
XIII. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
XIV. Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with.

2.2 The GDPR

Formally, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data, and repealing Directive 95/64/EC (General Data Protection Regulation), but most often shorted to "the GDPR". It was adopted in 2016 and came into effect in May 2018. The purpose of the GDPR is to update and modernise laws that **protect the personal information of individuals**, and to provide an equal level of protection across the EU. The GDPR is based around principles outlined through this document, namely of lawfulness, fairness and transparency; purpose limitation; data minimisation, accuracy; storage limitation; integrity and confidentiality, and accountability. The GDPR grants people many **rights**. When their data is processed, they must be provided with contact details for the data controller, information on the purposes of processing, how long the data will be stored, if they are obliged to provide data, sources of data, if the data will be transferred to third parties, information about any automated decision making and information about their other data protection rights. These include rights to request access to, correction or erasure of personal data, restriction of processing, to object to processing and to receive their data in a portable form. They also have the right to lodge a complaint about data processing with a supervisory body. To protect those rights, the GDPR empowers independent supervisory bodies (sometimes also called **Data Protection**

Authorities or Information Commissioners) to oversee compliance with the GDPR and to promote awareness of GDPR obligations and rights. These bodies work together as the European Data Protection Board. The GDPR also introduces significant **penalties** for non-compliance. Supervisory bodies can carry out investigations, issue warnings and reprimands to controllers, and impose fines up to €20 million or 4% of worldwide turnover for serious infringements of the GDPR.

3 ETHICS

At the outset of this section we introduce the readers to some key concepts:

- **Normative ethics** focuses on the content of human ethical behaviour and seeks to determine principles that, when followed, lead to ethically good behaviour, intentions, or outcomes.
- **Descriptive ethics** is the study of how people do in fact behave or how they do in fact categorise ethical behaviour.
- **Applied Ethics** attempts to deal with specific realms of human action and to craft criteria for discussing issues that might arise within those realms.[3]

As a descriptive fact, we know that ethical commitments are not homogenous across all cultures; there are different understandings of ethical principles, obligations, and transgressions. However, despite such factual differences, discussions concerning normative ethics can occur between groups of any background or particular experience owing to the fact that normative ethics is concerned with moral issues, values, principles, and practices.

Of relevance for D4FLY partners are the ethical values accepted by the European community. Its ethical identity is built on particular ethical commitments and contained in its human rights documents, such as the European Charter of Fundamental Rights. In developing technologies, D4FLY partners should be guided by the ethos that ICT cannot '**impair fundamental human rights and should contribute to the values they embody**,'[4] as such the use of ICT requires us to raise ethical questions.

3.1 Some of the issues partners should consider include:

I. The technology should respect a person's autonomy and dignity.

> **Autonomy** ought to be understood as an individual's capacity to self-govern, that is, to make decisions for him/herself.
>
> **Dignity** ought to be understood as being worthy of respect in virtue of being human.

To avoid violations of an individual's autonomy and dignity, researchers and partners can ask themselves:

- Does the person have a meaningful choice to participate in the collection of data/study/experiment/etc.? Can they opt out?
- Might he/she feel coerced or compelled and how can I identify and eliminate the circumstances leading to feeling coerced or compelled?

[3] Salloch, Sabine, Sebastian Wäscher, Jochen Vollmann, and Jan Schildmann. (2015). "The Normative Background of Empirical-Ethical Research: First Steps Towards a Transparent and Reasoned Approach in the Selection of an Ethical Theory". *BMC Medical Ethics*, Vol 16 Issue 20.

[4] Mordini, E., Wright, D., Wadhwa, K., De Hert, P., Mantovani, E., Thestrup, J., Van Steendam, G., D'Amico, A. & Vater, I., (2009). "Senior citizens and the ethics of e-inclusion". *Ethics and Information Technology*, Vol. 11 Issue 3, pp. 203–220

- Have all subjects been provided all relevant information and do they understand the information provided?

II. Consent has to be freely given and has to be informed.

III. The technology should not infringe upon anti-discrimination principles. Under Article 21 of the European Charter of Fundamental rights '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.'

IV. The technology should not cause harm. Harm is understood as both physical and psychological.

V. The technology should not exclude persons, e.g., those who are not competent ICT users.

VI. The technology should not isolate users and should be accessible/user-friendly.

VII. The technology should be economically and socially sustainable.

VIII. The vulnerable groups that may be affected by the technology. Vulnerable groups include: Children, pregnant women, elderly people, malnourished people, ethnic and gender minorities, migrants, those living with mental illness. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.

IX. The technology should not violate equality and fairness.[5]

X. The technology should not rely on algorithms that are biased, even implicitly biased, or that overly burden particular segments of the population.

3.2 Ethical opportunities

The preceding principles focus mainly on negative ethical risks. They identify principles, which when violated, reliably result in harming an individual or groups of individuals. In addition to these issues concerning ethical risks, partners also ought to consider issues concerning ethical opportunities. Partners can contemplate how technologies can promote values in addition to how they can avoid transgressing them. Whereas the former principles are presented as imperatives that ought not be violated, the following are presented as opportunities that partners can ask themselves.

I. Can the technology promote an individual's dignity and autonomy (e.g. perhaps by allowing the individual to perform tasks or make decisions they otherwise could not)?

II. Can the technology improve an individual's information thereby bolstering informed consent?

III. Can the technology promote equality among different sexes, genders, races, religions, and other backgrounds?

IV. Can the technology benefit users' wellbeing, or benefit the community?

V. Can the technology reach out to include oft-excluded segments of the population?

VI. Can the technology especially benefit vulnerable groups and individuals?

[5] A working definition of fairness is giving each his or her due. See John Rawls (2001) *Justice as Fairness: A Restatement*. Cambridge, MA: Harvard University Press.

VII. Can the technology promote equality and fairness?

3.3 Ethical concepts

A comprehensive list of all ethical concepts or a detailed discussion of their conceptual nuances fall outside the scope of this deliverable. However, the following table lists and provides a working definition of the concepts most relevant for D4FLY partners given the particular technologies under development and their foreseen implementation for the purposes of border security

TABLE 3-3 ETHICAL CONCEPTS

Ethical Concepts	Definition
Autonomy	The right, power, or condition of self-governance and self-determinism. Freedom from external control or coercion.
Beneficence	The ethical position whereby one attempts and is actually obligated to do no harm, remove harm, prevent harm, and actually do good.
Bias	The position whereby an individual shows partiality and prejudice and slanting an opinion in one direction or toward one group only.
Chilling Effect	The use of certain technologies can deter people from exercising their legitimate rights and freedoms.
Consequentialism	An ethical theory that claims that what is right or wrong is based on the good or bad consequences of an act.
Deontic ethics	An ethical theory that claims that the **morality** of an action should be based on whether that action itself is right or wrong under a series of rules, rather than based on the consequences of the action.
Dignity	Being worthy of respect in virtue of being human.
Equality (moral)	The principle that all people are of equal worth and are entitled to equal respect.
Implicit Bias	An implicit bias is any unconsciously-held set of associations about a social group and its members.
Moral dilemma	A situation in which a difficult choice has to be made between two courses of action, each of which entails transgressing a moral principle.
Non-maleficence	Moral principle that one should refrain from harming others.
Precautionary Principle	It is the responsibility of designers and engineers to establish that the proposed technology will not (or is very unlikely to) result in significant harm.
Rights	That which is due to individuals, based on core ethical principles. Rights create parallel duties on the part of others, or on society as a whole. So-called negative rights are rights of non-interference (e.g., with one's speech, conscience, associations), typically grounded in the principle of autonomy. Positive rights, by contrast, are rights of "recipience" (e.g., to education, health care), typically grounded in the principle of justice.

3.4 Why are these concepts important?

Becoming familiar with ethical concepts, human rights principles, and corresponding legislation can help avoid, though not completely eradicate, violations of individuals' dignity and equality. The following examples illustrate how stereotypes as well as algorithmic bias can produce unethical and illegal results.

- Despite the fact that black women who are US citizens are less than half as likely to be found carrying contraband as white women who are US citizens, US black women are nine times more likely than white women to be x-rayed after being frisked or patted down.[6]
- "Saeed Mohamed, a Somali-born Canadian citizen who, attempting to return to Canada from Kenya, was detained and denied the ability to return because border agents did not believe the photograph on her passport was indeed her, based on the appearance of Mohamed's lips. Despite possessing many citizenship documents, it was not until a DNA test on Mohamed's son revealed a match did government officials believe Mohamed was who she said she was, and what her travel documents indicated was Mohamed's body, that did not seem to 'match' the nationality on her passport, was read as suspect".[7]
- Studies show the algorithms of biometric facial recognition technologies reproduce racial and gendered stereotypes in the propensity for black women to be classified as men and Asian men to be classified as female.[8]

[6] Browne, Simone (2015). *Dark Matters: On The Surveillance of Blackness.* Durham, NC: Duke University Press, p. 132.
[7] Wilcox, Lauren (2017). "Gendered bodies in securitized migration regimes". *Handbook on Migration and Security*, edited by Phillippe Bourbeau, 87-104. Cheltenham, UK: Edward Elgar Publishing Limited, p. 97.
[8] Browne (2015) p. 111. Wilcox (2017) p. 97.

4 COMPLIANCE WITH LAWS, REGULATIONS, CODES AND GUIDELINES

In addition partners should be mindful of standards contained in, amongst others but not limited to:

- ISO/IEC 29100:2011
  - applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of personally identifiable information.
- Universal Declaration on Human Rights 1948
  - a comprehensive statement of inalienable human rights.
- European Convention on Human Rights 1953
  - The Convention established the European Court of Human Rights (ECtHR). Any person who feels his or her rights have been violated under the Convention by a state party can take a case to the Court. Judgments finding violations are binding on the States concerned and they are obliged to execute them.
- Charter of Fundamental Human Rights of the European Union 2009
  - enshrines certain political, social, and economic rights for European Union (EU) citizens and residents into EU law.
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980
  - OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation and, while upholding human rights, would at the same time prevent interruptions in international flows of data. They represent a consensus on basic principles which can be built into existing national legislation, or serve as a basis for legislation in those countries which do not yet have it.
- Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1980
  - The Convention for the protection of individuals with regard to automatic processing of personal data is a 1981 Council of Europe treaty that protects the right to privacy of individuals, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.
- General Data Protection Regulation 2016
  - The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. It is applicable only when personal data is collected or otherwise processed.

Trilateral will base the EPIA on the above standards and legislation, in addition to academic research concerning the ethics of border security, surveillance, and biometric data collection, and will guide partners through the process of adhering to elements of these standards and ethical insights.

The following GDPR protections and rights are particularly relevant to D4FLY, although more will be added as the framework is developed by Trilateral:

TABLE 4-1 SELECT GDPR RIGHTS/PROTECTIONS

Protections/Rights	Content
Right to be forgotten	Under Art. 17 data subjects will have a right to obtain erasure from the data controller without undue delay. This means that D4FLY research participants will have the right to have the record of their participation in the research deleted.
Data protection by design and default	Data controllers must include appropriate provisions for anonymisation, pseudonymisation and data minimisation.
Data security	Data controllers must implement technical and organizational measures to ensure an appropriate level of security for data, including the use of pseudonymisation and encryption, ability to ensure appropriate confidentiality and resilience of systems, ability to provide access to data in a timely matter in the event of an incident and undertaking regular testing of the security of the system.
Notification of data breaches	Authorities should be notified of any data breaches within 72 hours of their occurrence.
Processing personal data for research purposes	Appropriate safeguards must be in place when processing data for research purposes, including data minimisation, pseudonymisation and data security.

5 CONCLUSIONS

This deliverable has provided an overview of data protection, privacy and ethical concepts and regulations for the partners of D4FLY. It is the first step in an EPIA that will occur throughout the duration of the project. It fulfils the first deliverable, D3.1, of WP3.

REFERENCES

Browne, Simone (2015). *Dark Matters: On The Surveillance of Blackness.* Durham, NC: Duke University Press.

Kroener, Inga, and David Wright (2015). "Privacy Impact Assessment Policy Issues" in Artemi Rallo Lombarte and Rosario Garcia Mahamut (eds.) Hacia Un Nuevo Derecho Europeo De Protección De Datos. Towards A New European Data Protection Regime, Tirant lo Blanch, Valencia.

Mordini, E., Wright, D., Wadhwa, K., De Hert, P., Mantovani, E., Thestrup, J., Van Steendam, G., D'Amico, A. & Vater, I., (2009). "Senior citizens and the ethics of e-inclusion". *Ethics and Information Technology*, Vol. 11 Issue 3, pp. 203–220

Rawls, John. (2001) *Justice as Fairness: A Restatement*. Cambridge, MA: Harvard University Press.

Salloch, Sabine, Sebastian Wäscher, Jochen Vollmann, and Jan Schildmann. (2015). "The Normative Background of Empirical-Ethical Research: First Steps Towards a Transparent and Reasoned Approach in the Selection of an Ethical Theory". *BMC Medical Ethics*, Vol 16 Issue 20.

Wilcox, Lauren (2017). "Gendered bodies in securitized migration regimes". *Handbook on Migration and Security*, edited by Phillippe Bourbeau, 87-104. Cheltenham, UK: Edward Elgar Publishing Limited.

LIST OF TABLES

Table 3-3 Ethical concepts. 13
Table 4-1 GDPR Rights/Protections 14