Deliverable D4.3 First draft Criteria Catalogue and regulatory recommendations

WP4

Deliverable

Contract Number:	731711
Project Acronym:	TRUESSEC.eu
Project Title:	"TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe"

Document Identifier:	D4.3
Status:	Final version

Title of Document:	D4.3 First draft Criteria Catalogue and regulatory recommendations
Dissemination Level:	Public

Author(s):	Harald Stelzer (UNI Graz), Elisabeth Staudegger (UNI Graz), Hristina Veljanova (UNI Graz), Veronika Beimrohr (UNI Graz), Anna Haselbacher (UNI Graz)
Reviewed by:	Valentin Gibello (CERAPS)

Created on:	10 October 2017
Last update:	30 June 2018

CHANGE HISTORY

Date	Change	Author
10 October 2018	Input from ethics – laying the groundwork	Harald Stelzer, Hristina Veljanova
16 November 2018	Input from law	Elisabeth Staudegger, Veronika Beimrohr
18 January 2018	Merging ethics and law	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Veronika Beimrohr, Anna Haselbacher
23 January 2018	Merging ethics and law	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Veronika Beimrohr, Anna Haselbacher
27 January 2018	Defining the Core Areas of trustworthiness	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Veronika Beimrohr, Anna Haselbacher

8 February 2018	Defining the Core Areas of trustworthiness	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher
April 2018	Developing the Criteria Catalogue	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher
May 2018	Developing the Criteria Catalogue	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher
11 June 2018	Finalizing the deliverable	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher
15 June 2018	Internal review	Valentin Gibello (CERAPS)
25 June 2018	Addressing reviewer's comments	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher
30 June 2018	Final version	Harald Stelzer, Hristina Veljanova, Elisabeth Staudegger, Anna Haselbacher

Table of Contents

List of tables 5
Executive summary 6
1. Introduction 7
1.1. Goal 7
1.2. Methodology 8
1.3. Definition of key terms 9
2. Main findings of the ethical framework 10
3. Main findings of the legal framework 11
4. TRUESSEC.eu Core Areas of trustworthiness – Ethics and Law 13
4.1. Core Area: Transparency 14
4.2. Core Area: Privacy 15
4.3. Core Area: Anti-discrimination 16
4.4. Core Area: Autonomy 16
4.5. Core Area: Respect 17
4.6. Core Area: Protection 18
5. First draft Criteria Catalogue 18
5.1. Information 20
5.2. User-friendly consent 22
5.3. Enhanced control mechanisms 23
5.4. Privacy commitment 25
5.5. Unlinkability 26
5.6. Transparent processing of personal data 26
5.7. Anti-discrimination 27
5.8. Cyber security 29
5.9. Product safety 30
5.10. Law enforcement declaration 30
5.11. Appropriate dispute resolution 32
6. Recommendations 33
7. Conclusion 34
8. References 35

List of tables

Table 1: Developing the Criteria Catalogue ……..……..……..…... 8

Table 2: Attributes of trustworthiness from an ethical perspective ……....……. 10

Table 3: Overview of the most referenced CFR fundamental rights in secondary Union legislation ……... 12

Table 4: Core Areas of trustworthiness (Ethics and Law) ……..……. 14

Table 5: Criterion – Information ……..……..…….. 21

Table 6: Criterion – User-friendly consent ……..... 23

Table 7: Criterion – Enhanced control mechanisms ……..……..……. 24

Table 8: Criterion – Privacy commitment ……..…….. 25

Table 9: Criterion – Unlinkability ……..…….. 26

Table 10: Criterion – Transparent processing of personal data ……... 27

Table 11: Criterion – Anti-discrimination ……..……..…. 28

Table 12: Criterion – Cyber security ……..……..…….. 29

Table 13: Criterion – Product safety ……..…….. 30

Table 14: Criterion – Law enforcement declaration ……..……31

Table 15: Criterion – Appropriate dispute resolution ……..…... 33

Executive summary

The aim of the *Deliverable D.4.3 First draft Criteria Catalogue and regulatory recommendations* is to identify and clarify potential ethical and legal criteria that may be used to evaluate the trustworthiness of ICT products and service. For that purpose, we have developed a **First draft Criteria Catalogue** for security and privacy features of ICT products and services in regard to their trustworthiness as well as recommendations for the development of a European label for enhancing trust and security in Internet-based technologies and services. The Criteria Catalogue has in its core the European values and fundamental rights.

These are the steps we took and the main findings we have formulated as part of this deliverable:

1. Based on the support studies carried out in the first year of the project as well as based on some interdisciplinary work, we have agreed upon six **Core Areas**, which make up the basis of the TRUESSEC.eu Criteria Catalogue. These include: transparency, privacy, anti-discrimination, autonomy, respect and protection. The input we have provided in this report comes only from ethics and law, although we have also started to involve the other disciplines and partners.
2. The six Core Areas helped us and guided us in the search of **criteria** that may be used to evaluate the trustworthiness of ICT products and services. So far we have identified eleven criteria.
3. To each criterion we have assigned corresponding **indicators**, which should tell us to what degree a criterion is fulfilled. The list of criteria and indicators is not complete since with the fast pace of technological advancement it is likely to expect that the need may arise to include additional criteria. Nevertheless, the eleven criteria provided in the Criteria Catalogue can be considered as the fundamental ones.
4. We have also formulated **recommendations** to strengthen the role of fundamental rights and European values in the further development of ICT products and services.

All these findings will be further incorporated in WP7, namely in the development of the transdisciplinary Criteria Catalogue and the TRUESSEC.eu recommendations for trust-enhancing label.

1. Introduction

1.1. Goal

In light of the ever-increasing use of and dependence on ICT products and services as well as following the efforts of the European Union to boost the Digital Single Market and build a European data economy, there is a clear need to build a reliable and trustworthy ICT infrastructure that will safeguard fundamental rights. Building such an infrastructure will address and help overcome one very common challenge: Everyone wants to enjoy the numerous benefits offered by new and emerging technologies. However, it is well-known that consequences of innovations can conflict with fundamental rights and European values and hence strongly undermine the trust in technology and businesses.

This report presents *Deliverable D.4.3 First draft Criteria Catalogue and regulatory recommendations*. The main goal of the report is to gather the findings of **D.4.1 Support Study: Legal Analysis**[1] and **D.4.2 Support Study: Ethical Issues**[2] and based on these findings to provide a first draft, a first collection, of multidisciplinary criteria that can be used to evaluate the trustworthiness of ICT products and services. This closely relates to one of the main objectives of the TRUESSEC.eu project, which is to provide a **Criteria Catalogue** for security and privacy features of ICT products and services and **recommendations** for the development of a European label for enhancing trust and security in Internet-based technologies and services. In doing so, the project brings us a step closer to the goal of protecting fundamental rights and promoting a flourishing digital society based on citizens' trust.

In accordance with the TRUESSEC.eu project proposal we have taken a user-centred approach.[3] With all this in mind, the report has a twofold purpose: (i) to provide a first draft of multidisciplinary criteria and recommendations, and (ii) to lay the foundation of and further guide the input for WP7. The report's findings are intended for various stakeholders including end-users, service providers, businesses, industry etc.

[1] GIBELLO, V, "TRUESSEC.eu - Deliverable D4.1. Support Study: Legal Analysis", and BEIMROHR, V, "Annex to Deliverable D4.1. Overview over the Legal ICT-Framework", 2017, published on https://truessec.eu/library.
[2] STELZER, H./ VELJANOVA, H, "TRUESSEC.eu - Deliverable D4.2 Support Study: Ethical Issues", 2017, published on https://truessec.eu/library.
[3] Proposal for TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe, p. 14

1.2. Methodology

As already mentioned, the aim of the report is to provide the first draft of Criteria Catalogue and regulatory recommendations. In order to do so, we have taken the following steps:

Table 1: Developing the Criteria Catalogue

1. We have used the findings from the legal and ethical support studies (**D.4.1 Support Study: Legal Analysis** and **D.4.2 Support Study: Ethical Issues**) where the key pillars of trustworthiness have been identified from a legal and ethical perspective. These findings form the basis of our work on the Criteria Catalogue.

2. We have also taken into account the **Annex to D.4.1: Overview over the Legal ICT-Framework**. It is based on two pillars, namely the **European values** as stated in Article 2 of the Treaty of the European Union and the **European fundamental rights**. Respect for human dignity, non-discrimination, justice, freedom and equality are the main European values we have considered as they play an important role in the context of ICT products and services. This mapping served as the fundament for our research and interdisciplinary discussion.

3. Based on both the European values/fundamental rights, the findings from the support studies as well as some interdisciplinary work with the other disciplines in the TRUESSEC.eu project, we have identified six common **Core Areas** of trustworthiness, which an ICT product or service has to respect in order to be considered trustworthy.

4. Since the Core Areas of trustworthiness are pretty abstract, they were further concretized into eleven **criteria**. The list of the criteria we have provided is based upon our reflections on what is relevant for the context of ICT and especially for increasing trustworthiness.

5. In order to identify whether a criterion has been met, we have formulated corresponding **indicators**. When compared to the Core Areas and criteria, the indicators operate on a more concrete level and hence set the ground for the operationalization process and their translation into the technological domain, which will be part of WP7.

1.3. Definition of key terms

Core Areas

The very aim of the Core Areas is to guide us in drafting the Criteria Catalogue. They reflect the values that ought to be taken into consideration in both the design and use of ICT, which explains their level of abstractness. Moreover, the Core Areas serve as an orientation map in the selection of the criteria and tell us what criteria are needed so that these Core Areas can be addressed. Additionally, doing interdisciplinary work has imposed the need to come up with such a common denominator, which is broad enough to encompass interdisciplinary considerations and specific enough to include context-related aspects. The defined six Core Areas are the result of such an interdisciplinary work, which includes the input not only from ethics and law but also from other disciplines represented in the TRUESSEC.eu project, namely, sociology, business and technology. Additionally, the list of the Core Areas was presented and discussed at the TRUESSEC.eu Advisory Board Meeting in February 2018 in London. The feedback has been accordingly implemented.

Criteria

Criteria represent standards by which the trustworthiness is compared or judged. In our report, the aim of the criteria is to tell us what requirements an ICT product or service should meet in order to be considered trustworthy, that is, the main aim of the criteria is to evaluate the trustworthiness of ICT products and services. In that way, the criteria also demonstrate whether the Core Areas have been met.

Indicators

Indicators serve as tools that show whether the criteria have been met. There are usually several indicators that relate to one criterion. Some of them are binary, which means they are either fulfilled or not, others come in degrees. Not all indicators are measurable. Indicators need to be operationalized.

Users

By this term we refer to end-users (unless otherwise specified), that is, individuals who interact with ICT for non-enterprise purposes. Making such a distinction is highly relevant since individuals or even businesses using ICT for enterprise purposes may have different expectations in terms of, for example, privacy compared to those using it for non-enterprise ones. Moreover, in our context the term ‘users’ encompasses both data subjects and consumers.

2. Main findings of the ethical framework

The ethical analysis conducted as part of **D.4.2 Support Study: Ethical Issues** resulted in the identification of the central elements and requirements necessary for building trustworthy ICT products and services from a normative perspective. This was achieved by a three-step approach: (i) identification of the fundamental concepts relevant for the TRUESSEC.eu project, (ii) identification and analysis of the fundamental ethical issues and challenges in the context of new services and technologies, and (iii) normative analysis of potential conflicts between values, rights and interests.

The fundamental concepts have been identified in relation to the two leading concepts relevant for the TRUESSEC.eu project, trust and trustworthiness. These include privacy, autonomy and informed consent, security, transparency, responsibility/accountability, and justice. These concepts have also been considered as attributes of trustworthiness because they indicate what is relevant from an ethical perspective when designing and using ICT. The six attributes have been considered as the starting point for further considerations on the development of the TRUESSEC.eu Criteria Catalogue for trustworthy products and services.

Attributes of trustworthiness from an ethical perspective - D.4.2[4]	
Privacy	**Transparency**
Autonomy and Informed consent	**Responsibility and Accountability**
Security	**Justice**

Table 2: Attributes of trustworthiness from an ethical perspective

The ethical issues that have been identified and elaborated in the second step of the support study revolve around the six attributes of trustworthiness. The most common issues include loss of control over one's personal data, consent problems (i.e. lack of informed consent), security breaches, lack of transparency with users' data, too wide informational asymmetry between users and ICT providers, cases of data-based discrimination and biased decision-making etc.

[4] STELZER / VELJANOVA, "TRUESSEC.eu - Deliverable D4.2 Support Study: Ethical Issues", 2017, p.7, published on https://truessec.eu/library.

As to the third aspect of the support study, the normative analysis focused on multiple stakeholders that directly or indirectly partake in or are affected by ICT such as developers, providers, users. The analysis has shown that the mutual interaction among these stakeholders may easily result in conflicts of interests and/or rights among them or within a single group. Examples of some of the most common conflicting situations are: users' data privacy vs the social and economic value of data-driven innovation, users' data privacy vs businesses' profit interests based on users' data, users' data privacy and security vs user-friendliness of a product/service, transparency vs data/system security. The challenge in overcoming such conflicts is even greater given that they cannot always be solved by technological means and/or by taking a balanced approach. Trade-offs are one possible answer to such cases, however, one has to be careful with this approach since trade-offs demand that we prioritize one thing over the other. It is important that such prioritization is justified.

3. Main findings of the legal framework

ICT services and products also need to respect European values and fundamental rights in order to be called trustworthy. Article 2 of the Treaty of the European Union clearly states the values common to the Member States such as respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including minorities.[5] These values form one pillar of the TRUESSEC.eu framework. The other pillar consists of the European fundamental rights as laid down in the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights (CFR).

The Annex to D.4.1 identified the following fundamental rights as especially relevant to the Digital Single Market:

CFR fundamental right	**Number of references**
Art 8 – Protection of personal data	18
Art. 7 - Respect for private and family life	17
Art. 11 - Freedom of expression and information	10
Art. 47 - Right to an effective remedy and to a fair trial	9

[5] Article 2 of the Treaty on European Union: "*The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail*."

Art. 17 - Right to property	7
Art. 16 - Freedom to conduct a business	6
Art. 21 - Non-discrimination	4
Art 38 - Consumer protection	4
Art. 48 - Presumption of innocence and right of defence	4

Table 3: Overview of the most referenced CFR fundamental rights in secondary Union legislation

The Annex to D.4.1 provided in a first step a map to the current European Union legal framework, which governs ICT product manufacturers and service providers. This map illustrated the extensiveness of this legal landscape, so far over sixty potentially relevant secondary Union legislative acts have been identified. As part of the EU legal framework on ICT a particularly high number of secondary legal acts can be observed among the area of consumer protection. The right to protection of personal data (Article 8 CFR) and respect for private and family life (Art 7 CFR) are the two most referenced CFR fundamental rights in the secondary EU legislation in the field of ICT.

The legal analysis in D.4.1 provided an in-depth analysis focusing on legislation pertaining to privacy (personal data protection), security and consumer protection. These areas were found fundamental for trust in ICT. The resulting legal corpus is the basis for the Criteria Catalogue and can be further used by trust marks operators. Moreover, the analysis of the legal framework was further translated into technical requirements, which are ultimately meant to build trust in ICT products and services. It should be noted that by including law and legal considerations in the development of the Criteria Catalogue the idea is not to reduce it to compliance and law enforcement but rather to stress them as important factors in increasing trustworthiness. This is further strengthened by the fact that in the Criteria Catalogue we have also included aspects that go beyond the law such as alternative dispute resolution.

4. TRUESSEC.eu Core Areas of trustworthiness – Ethics and Law

As already elaborated, based on the findings from two support studies, taking into account the European values and fundamental rights as well as following joint work with the other disciplines represented in the TRUESSEC.eu project, six Core Areas have been agreed upon that set the stage for the search of the multidisciplinary criteria. At this stage, the Core Areas and the table displayed below represent the reflections of only ethics and law. These will be further developed within **D7.2 Cybersecurity and privacy Criteria Catalogue for assurance and certification** where the input from the other disciplines (sociology, business and technology) will be included.

Ethics	Law	TRUESSEC.eu Core Areas
Transparency relates to two aspects: ○ providing clear and sufficient information about the products and services; ○ providing information to users regarding activities with their personal data.	**Transparency** as in information duties laid down in the GDPR, the Directive on consumer rights or the e-commerce Directive. With respect to personal data, transparency is one of the core principles of data processing (Article 5 GDPR).	➔ **Transparency** The ICT product or service is provided in line with information duties regarding personal data processing and the product/service itself.
Privacy stands for the individual's claim to control the access to and use of her personal information. The idea behind it is that people have the claim to determine who knows what about them thus preventing unjustified interferences by others.	**Privacy** as preserving respect for private life (Art 7 CFR) and the protection of personal data (Art 8 CFR) in the context of ICT. This includes the GDPR as well as Directive 2002/58/EC.	➔ **Privacy** The ICT product or service allows the user to control access to and use of their personal information and it respects the protection of personal data.
Justice relates to different aspects such as: ○ anti-discrimination ○ fairness ○ distributive justice.	**Justice** as the remedies against the unjustified use of force by the state, such as the right to a fair trial (Art 47 CFR) and the presumption of innocence (Art 48 CFR). This meaning further entails equality before the law (Art 20 CFR) and anti-discrimination (Art 21 CFR).	➔ **Anti-discrimination** The ICT product or service does not include any discriminative practices and biases.

Autonomy can be seen as relating to: ○ capacity for self-determination -> as the capacity/ability to lead one's life and make decisions based on one's beliefs, values and motives; ○ possibility (freedom) to act upon one's judgment regarding aspects that affect one's life.	**Autonomy** as preserving freedoms, such as freedom of thought, conscience and religion (Art 10 CFR), freedom of expression and information (Art 11 CFR), freedom to conduct a business (Art 16 CFR) and the right to (intellectual) property (Art 17 CFR). Within the GDPR it further includes the right to data portability (Art 20 GDPR).	➔ **Autonomy** The ICT product or service gives users the opportunity to make well-informed decisions free of coercion.
Under the concepts of **responsibility and accountability** fall the following aspects: ○ moral agency (*Who/What* is to be held morally responsible?); ○ attribution of responsibility (backward looking); ○ prevention (forward looking – responsibility as duty).	**Lawfulness** as in lawful conduct and taking preventative care in accordance with the law, especially when dealing with consumers (Art 38 CFR). With respect to personal data, lawfulness is one of the leading principles of data processing (Article 5 GDPR) and therefore well elaborated in detail (Article 6 GDPR).	➔ **Respect** ICT products or services are to be provided in accordance with the legitimate expectations related to them.
Security is understood as freedom from (physical, psychological, economic etc.) harm and protection of one's rights, liberties.	**Security** as the protection from harm, such as the right to liberty and security (Art 6 CFR) as well as the right to the integrity of the person (Art 3 CFR) and the right to life (Art 2 CFR). Regarding data processing, security is the core issue of the NIS-Directive and enacted in the GDPR as well.	➔ **Protection** ICT products and services are provided in accordance with safety and cybersecurity standards.

Table 4: Core Areas of trustworthiness (Ethics and Law)

4.1. Core Area: Transparency

From an ethical perspective, *transparency* can be considered as the key concept in the ICT discourse as it serves as a mean to realizing other Core Areas such as privacy, anti-discrimination, autonomy, respect and protection. Furthermore, *transparency* is also even more

important due to the wide informational asymmetry that exists between individuals and providers of ICT products and services.

From a legal perspective, *transparency* builds one main requirement of trustworthiness and is legally assured by information duties. Its enforcement is particularly fuelled by GDPR's severe monetary fines. In accordance with the ethical point of view, *transparency* does not constitute a stand-alone area but is rather interconnected with others like autonomy or anti-discrimination.

The common Core Area *transparency* reflects the understandings of the two disciplines by having information in its main focus. In this regard, the Core Area *transparency* evolves around the fulfilment of information duties related to personal data processing. This would help to narrow down the existing informational gap and give users clearer answers to question regarding their personal data.

4.2. Core Area: Privacy

With data being the main 'currency' of today's ICT society, this has made *privacy* one of the most pressing ethical issues. *Privacy* has a normative dimension and can be understood as an individual's claim to exercise control over one's data. Ethical concerns often arise when individuals lack answers as to activities with their personal data.

Legally speaking, while aiming to strengthen user's trust, *privacy* plays an essential role, which is emphasised by the fact that the right to protection of personal data (Article 8 of the EU Charter of Fundamental Rights - CFR) and respect for private and family life (Article 7 CFR) are the two most referenced CFR fundamental rights in secondary EU legislation regarding ICT.

When users are provided with relevant information, this sets the ground for them to act out control over their data. On the one hand, users must be able to make decisions regarding their personal data, on the other hand, providers must respect those decisions. The latter is a striking point, as providers have commercial interests in processing as many data as possible. Considering the economic relevance of data and the emerging Data Economy, it is crucial to ensure the protection of personal data. This includes considering aspects of *privacy* throughout the design and development of an ICT product or service (privacy by design) as well as offering the privacy settings at a high level of privacy protection (privacy by default).

4.3. Core Area: Anti-discrimination

From an ethical perspective, one of the greatest concerns in the domain of *justice* arise around practices of data-based discrimination and biased-decision making. The concerns pertain to cases where decisions are made based on individual's data that may lead to unjust treatment, bias or exclusion of some individuals or groups from certain opportunities. Further aspect, which arises in the context of ICT, is the fair distribution of benefits and costs of ICT among members of society.

Legally considered, the requirement regarding justice means that besides ensuring rights and freedoms to individuals, one must also be provided with efficient remedies in order to effectively enforce them (TITLE VI CFR: JUSTICE). From a broader legal understanding, justice includes equal treatment of individuals and thus *anti-discrimination* (TITLE III CFR: EQUALITY). Within the ICT context, *anti-discrimination* is the key term to consider, meaning humans must not implement any illegal discriminative features or processes in the ICT product or service. Thus, the GDPR explicitly governs lawfulness as a main principle (Article 5) e.g. regarding profiling as defined in Article 4(4).

In the efforts to merge the ethical and legal understandings of justice into one common concept that could accommodate both disciplines, we have arrived at the Core Area *anti-discrimination*. *Anti-discrimination* is one aspect that has great relevance for both ethics and law particularly in the context of ICT. The need to formulate such a core area stems from the fact that discrimination concerning ICT products and services is present and is very often hidden in decision-making carried out by algorithms and self-learning systems. This particularly relates to cases where parameters are included in the decision-making process, which go beyond the scope of the service or product in question.

4.4. Core Area: Autonomy

Privacy is closely related to the concept of *autonomy* since the first creates the conditions for the exercise of the latter. One way to reinforce *autonomy* is through informed consent which stands for the possibility of being informed about data processing activities and having the freedom to act upon one's decisions regarding data. Cases where informed consent lacks are ethically problematic since they directly undermine the very essence of *autonomy*.

Autonomy constitutes another normative requirement for trustworthiness legally referring to the individual's guaranteed fundamental freedoms (TITLE II CFR: FREEDOMS; including e.g. respect for private and family life and protection of personal data as well as the freedom to

conduct business). As it is likely that between the preserved freedoms and other guaranteed fundamental rights conflicts will arise, the aim is to find a balance between them. Considering ICT, *autonomy* results in the user's freedom to freely make decisions, thus being respected by the ICT product or service.

The Core Area *autonomy* summarizes well both the ethical and legal considerations. Having access to and using various ICT products and services brings up one very central issues, that is, the need for users to be given the opportunity to make decisions regarding their personal data. These decisions need to be well-informed and free of manipulation and coercion.

4.5. Core Area: Respect

Responsibility and *accountability* are further concepts that play an important role, in particular due to the possible impact of ICT on individual and societal level. This especially includes consequences that are unanticipated and hard to foresee. From a philosophical perspective, *responsibility* and *accountability* can be observed in a three-fold manner: (a) in terms of moral agency: *Who/What* is to be held morally responsible?[6], (b) in terms of attribution: backward-looking, where the morality of someone's actions is inspected, and (c) in terms of prevention: forward-looking, where responsibility is understood as a duty, namely, who should do *what*.

Legally speaking, the requirement of *respect* here is referred to as lawful behaviour based on accountability, responsibility and liability within the field of consumer protection. This view is supported by the fact that the EU legal framework on ICT has a high number of secondary legal acts that are within the area of consumer protection law. Moreover, within the GDPR accountability builds the basic approach of European data protection law (Article 5(2)).

The Core Area *respect* presents a transition from discipline-related understanding to a transdisciplinary one. It embodies the idea that based on societal, legal and ethical frameworks there are certain duties that arise for ICT providers that ground legitimate expectations on the side of users when dealing with ICT products and services. Legitimate expectations have three main hallmarks: they are predictive, prescriptive and justifiable.[7] In the ICT context, this would suggest that users form expectations on what ICT providers will and should do or not do, how they will and should operate, whereby these expectations are justifiable, that is, users have epistemic justification or warrant for forming them in the first place. Example of such legitimate expectations is that ICT providers respect users' rights and freedoms.

[6] This goes back to the discussion whether technology, apart from human beings, can be held responsible. For more see STELZER/ VELJANOVA, "TRUESSEC.eu - Deliverable D4.2 Support Study: Ethical Issues", 2017, published on https://truessec.eu/library.

[7] Alexander Brown elaborates on the concept of legitimate expectations in his paper "A Theory of Legitimate Expectations", *Journal of Political Philosophy* vol. 25 no. 4 (2017): 435-460.

4.6. Core Area: Protection

The reason why *security* is assigned great importance when discussing ICT is more than obvious. *Security* can be considered as the foundation for the realization of some other areas such as privacy. For example, one of the precondition to guaranteeing privacy is the existence of a solid security infrastructure. In that sense, one way to analyse security issues in an ICT context is as the security of data and systems where data reside. However, from an ethical perspective, *security* can also be understood in a much broader sense as a freedom from harm and protection of rights and liberties.

From a legal perspective, *security* means protecting individuals from harm, with the fundamental right to human dignity and life (TITLE I CFR: DIGNITY). In the ICT context, this implies actively providing protection to users by preventing them from harm through fulfilling safety and cybersecurity standards. Again, the GDPR states special duties with respect to data security. Data protection law is now accomplished by the NIS-Directive.

The considerations of both ethics and law seem to have in its focus the protection of individuals against any harms as well as the protection of their rights and liberties. This has led us to formulate the Core Area *protection* as the sixth core area. In the context of ICT, *protection* relates to both safety and security thus encompassing risks of physical injury or damage and risks related to data such as unauthorized access, identity theft etc. In order to enable solid level of protection, compliance with already established safety and cybersecurity standards is essential. The aim is to hinder any harms that may be caused as a result of using ICT in the first place.

5. First draft Criteria Catalogue

The aim of the First draft Criteria Catalogue is to identify and clarify the ethical and legal criteria that constitute necessary conditions for establishing the trustworthiness of ICT products and services. Having determined the six Core Areas of trustworthiness, the way is paved for the identification of the criteria. The six Core Areas represent the foundation of the Criteria Catalogue since they are the guidelines in our search for the criteria.

The Criteria Catalogue is presented in a tabular form. To each criterion corresponding indicators have been assigned that show to what degree the criterion is fulfilled. The order of the criteria does not reflect their importance but merely displays a coherent and easy way to follow them. In order to ensure that all relevant criteria have been identified we have crosschecked them with the six Core Areas. For that purpose, we have used a colour system. We have assigned a specific

colour to each Core Area, which helped us to assess the degree to which a concrete criterion addresses and fulfils each of the six Core Areas. In order to check this, we have added a separate column to the left of each criterion, which we have named **'Trustworthiness enhancer'**. This column is divided into six sections representing the six Core Areas. Each section consists of three boxes where a colour can be applied that would show the degree to which we believe that a criterion addresses each Core Area. Depending on the degree, one could apply colour to one, two or three boxes, with three meaning the criterion fully addresses and meets the particular Core Area. At this stage, it is not necessary to assign each Core Area a list of criteria as long as we can make sure that the identified criteria address all the Core Areas to a satisfactory degree.

The criteria themselves can stand in several relations. While some criteria can be seen as knock-out criteria, meaning that, if not met to a certain satisfactory level, a product or service cannot be considered trustworthy, others come in degrees in terms of their fulfilment. This leaves space for certain prioritization among the criteria themselves. It should also be noted that we have renounced from talking about absoluteness in terms of the criteria. This is out of pragmatic reasons and due to the fact that it is not feasible and realistic to guarantee absolute fulfilment of a single criterion. For instance, it is impossible to guarantee or demand absolute privacy or transparency but rather a reasonable and satisfactory level of it. In order to establish how that satisfactory level would look like, we need to determine thresholds for the Core Areas and the criteria. This would demand further work and elaboration, which we will not be able to provide in this report.

In this first draft we have identified the following eleven criteria:

- Information
- User-friendly consent
- Enhanced control mechanisms
- Privacy commitment
- Unlinkability
- Transparent processing of personal data
- Anti-discrimination
- Cyber security
- Product safety
- Law enforcement declaration
- Appropriate dispute resolution

In its latest strategies and particularly as part of the Digital Single Market strategy, the European Union clearly aims at promoting the data economy, free flow of data and information society where personal freedoms and fundamental rights are respected. In the context of ICT, limitation to the collection and use of personal data constitutes an important trustworthiness aspect, nevertheless, since limitation is sufficiently covered by the GDPR via the data minimization and purpose limitation principles, it is not necessary to include it as a separate criterion in the Criteria Catalogue.

The provided list of criteria is not complete and can vary depending on the ICT product or service in question. Moreover, with the fast pace of technological advancement it is likely to expect that the need may arise to include additional criteria. Nevertheless, the eleven criteria provided in the Criteria Catalogue can be considered as the fundamental ones.

5.1. Information

Information is undoubtedly the first step in enhancing the trustworthiness of ICT products and services. Having the relevant information allows one to make informed decisions and it also creates a climate of openness, transparency and responsibility. Information is a necessity since it helps answer basic questions such as who does what in what way etc. In that regards, there are two main aspects that ought to be taken into account so that this criterion fulfils its purpose: (a) the content and (b) the form in which information is provided.

(a) Content relates to *what* the user is informed about and whether the provided information is relevant and useful for the particular context. Overloading users with unnecessary and too much information would only bring more difficulties in understanding the issue that is the subject of the information in the first place. In the context of ICT, users need information on activities with their personal data. In order to determine what these activities are, we have framed them in six WH-questions, each pertaining to a particular aspect of activities with personal data.

(b) The second aspect, the form, relates to *how* the information is provided to the user. Information must be easily accessible and easy to understand, using a simple language and should be no longer than one page. This gives users the essential information they require in a less time-consuming manner.

This criterion addresses directly or indirectly all six Core Areas, which further adds to its value.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Information**	i. Information is provided about: a. What data is collected? b. Who collects and processes the data? c. How long will the collected data be stored? d. For what purpose is the data collected and used? e. How will the data be processed? f. What are users' rights? o right to access o right to rectification o right to erasure ('right to be forgotten') o right to restrict and/or object processing o right to data portability o right not to be subject to a decision based solely on automated processing. ii. Information is provided: a. in a plain language b. in a way that is easy to understand c. clearly visible and easy to locate d. in a user-friendly manner e. relevant to the context f. as long as necessary and as short as possible (e.g. in a form of one pager). iii. Information is provided free of charge.

Table 5: Criterion – Information

5.2. User-friendly consent

With information being the first criterion and first step towards enhancing the trustworthiness of ICT products and services, the way is paved for the next criterion, which we named *'user-friendly consent'*. As the name itself suggests, this criterion relates to two important aspects: (a) the act of consenting (b) in a user-friendly manner.

In the words of the GDPR consent means *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.[8] With respect to trustworthiness, the issue of consent firstly addresses communication between providers and users on a par: Users consent freely to something they know and understand (→ information). They are treated as esteemed contractual partners.

Therefore, consent calls for specific attention due to the high level of uncertainty, risk as well as the lack of transparency that exist in the digital realm. Furthermore, consent as such embodies the idea of users' empowerment and possibility for making decisions regarding one's personal data. Consent is about having the relevant and sufficient information provided in a timely manner so that a decision can be made based on that information. This confirms that information presents a precondition to consent. Furthermore, consent demands the active participation of users, which may come in various forms such as ticking off a box. It also goes hand in hand with the possibility of withdrawing already given consent as well as opting-out from data processing in the first place.

This type of consent addresses and overcomes problems that arise with other types of consent such as implied consent (where the inaction of the user is interpreted as a sign of consenting to data processing), conditional consent (where the provision of the service and/or the use of the product is conditional upon user's consent to the processing of personal data that is not necessary for the provision of the service/use of the product) or cases where no consent is offered at all but only information is provided regarding data processing activities.

Since in the essence of this criterion lies the idea of empowering users and enabling them to make decisions, it can be argued that in that way it clearly addresses few of the six Core Areas, namely, transparency, privacy, autonomy and respect.

[8] Article 4 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency, Privacy, Anti-discrimination, Autonomy, Respect, Protection	**User-friendly consent**	i. All relevant information is provided in a clear, easily understandable, clearly visible and unambiguous way. ii. The information is provided in a timely manner, for instance, prior to data processing. iii. Consent is demanded by active participation of the user such as in the form of ticking off a box. iv. The silence or inaction of the user is not interpreted as consent. v. Users are given the option to opt-out from data processing. vi. Users are given the option to withdraw previously given consent. vii. User-friendly consent is in accordance with consumer protection requirements. viii. Provision of the service and/or the use of the product is not conditional upon user's consent to the processing of her personal data, which is not necessary for the provision of the service and/or for the use of the product.

Table 6: Criterion – User-friendly consent

5.3. Enhanced control mechanisms

Assuming greater control over one's personal data implies the existence of corresponding mechanisms and processes. The *'enhanced control mechanisms'* criterion ensures that there are such mechanisms and processes in place. These mechanisms relate to several important aspects such as having the possibility to have one's personal data corrected, request the deletion of

personal data, object to the processing of personal data as well as the possibility for data portability.

The criterion addresses all Core Areas.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Enhanced control mechanisms**	i. Users are given the opportunity as well as fast, easy and efficient means/processes to: a. have their personal data corrected, if it is inaccurate or incomplete; b. request the deletion of personal data (where applicable); c. restrict and/or object to processing of personal data (under specific circumstances). d. exercise the possibility for data portability. ii. Information published by the user is handled according to clear, transparent and binding guidelines. a. The provider of the ICT product and service follows and abides by these guidelines. iii. All settings and parameters offered to the user are set by default to the least privacy-invasive state as regards data protection principles.

Table 7: Criterion – Enhanced control mechanisms

5.4. Privacy commitment

The criterion *'Privacy commitment'* has the purpose to further strengthen privacy in the digital realm. This criterion focuses on two essential aspects:

(a) The existence of a commitment to the GDPR. Since the GDPR currently presents one of the main pillars of data protection within the EU, an ICT provider showing its dedication to comply with GDPR's principles in a form of a declaration can be a relevant factor in increasing trustworthiness.

(b) Carrying out data protection impact assessment is a further sign of commitment of an ICT provider to privacy and data protection.

This criterion addresses all Core Areas: privacy, transparency, anti-discrimination, autonomy, respect and protection.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Privacy commitment**	i. The ICT provider clearly states its commitment to the GDPR in form of a declaration. ii. The ICT provider carries out a data protection impact assessment for data processing.

Table 8: Criterion – Privacy commitment

5.5. Unlinkability

The concept of unlinkability is constituent part of reinforcing and protecting privacy. It aims at ensuring that personal data cannot be liked to other personal data within or outside of a domain. Unlinkability gets its value from the fact that it enables the collection and sharing of data without jeopardizing the data itself and the privacy of those to whom the data belongs. Balancing these two aspects can very often prove to be challenging, which reaffirms even more the relevance of the concept and the need to include it in the Criteria Catalogue.

TRUSTWORTHINESS ENHANCER				CRITERION	INDICATORS
Transparency				**Unlinkability**	i. Where applicable, appropriate methods are used to ensure unlinkability of personal data such as: a. pseudonymisation b. anonymization c. undetectability etc.
Privacy					
Anti-discrimination					
Autonomy					
Respect					
Protection					

Table 9: Criterion -Unlinkability

5.6. Transparent processing of personal data

This criterion predominantly relates to the Core Area transparency, even though other Core Areas are addressed by it such as privacy. Following the recent Cambridge Analytica scandal, it was made apparent that the need for transparency is even greater in times of such privacy breaches and great uncertainty regarding personal data. One way to deal with issues like these

is to advocate for a transparent data processing. This would demand providing information about data processing, categories of data that are being collected and used as well as any tools that are being used as part of the processing activities.

Transparency is one of the pillars towards building more trustworthy ICT products and services. With that in mind, it is a constituent part of trustworthy data processing. Apart from its relation to transparency, this criterion is even more important as it also addresses further Core Areas like privacy and respect.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency, Privacy, Anti-discrimination, Autonomy, Respect, Protection	**Transparent processing of personal data**	i. Relevant information is provided regarding processing of personal data in an easy and understandable way. ii. The categories of data used for processing are disclosed/revealed. iii. Those who process data specify which tools they use (e.g. data profiling or scoring) iv. It is also specified whether the collected data is shared with third parties that further process the data.

Table 10: Criterion – Transparent processing of personal data

5.7. Anti-discrimination

Cases of data-based discrimination and biased decision-making constitute one of the most common ethical and legal issues that arise in relation to ICT. As a result of the increased automation of the decision-making processes and the use of algorithms, there is a great

uncertainty about the parameters that are embedded in an algorithm and that form the basis for making decision in the first place. However, it should be emphasized that cases of positive discrimination (e.g. when women are prioritized over men in order to decrease gender gap and hence gender plays an important parameter in decision-making) or when it is simply part of a business model (e.g. if a company produces and sells products intended only for women it cannot be argued that it discriminates men) do not lie in the focus here. Of interest are cases that are particularly alarming and problematic, that is, cases where parameters such as age, race, ethnicity, income etc., are included in the decision-making even though they do *not* bear any relevance for providing a particular service or product. In that sense, advocating for greater algorithmic transparency and fairness is something that can undoubtedly contribute to increasing trustworthiness of ICT.

TRUSTWORTHINESS ENHANCER				CRITERION	INDICATORS
Transparency				**Anti-discrimination**	i. Profiling techniques are used in accordance with legal and ethical standards. ii. Information about profiling techniques and algorithms is available to users. iii. Reasons not related to the product or service are not included in the decision-making processes.
Privacy					
Anti-discrimination					
Autonomy					
Respect					
Protection					

Table 11: Criterion – Anti-discrimination

5.8. Cyber security

The two already mentioned criteria *'Unlinkability'* and *'Privacy commitment'* made clear that the protection of privacy has a great value in the trustworthiness discourse. However, privacy cannot be guaranteed without the existence of a solid security infrastructure, which would serve as a shield against any security breaches and cases of identity theft, unauthorized access of third parties etc. In that sense, cyber security can be considered as the other side of the same coin. In order to ensure that sufficient cyber security measures exist, an ICT provider needs to comply with relevant ISO standards, use state of the art security practices as well as timely inform users in cases of occurred security breaches.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Cyber security**	i. Use of state of the art security practices. ii. The ICT product or service is compliant with relevant ISO standards. iii. Adequate information is timely provided for already occurred security breaches.

Table 12: Criterion – Cyber security

5.9. Product safety

A great deal of ICT products and services that users use on a daily basis can have unwanted consequences in the physical domain, which may also result in inflicting injuries and harming users. One way to guarantee the safety of an ICT product is for the ICT provider to provide necessary and relevant information to users regarding the functionality and quality of the product as well as to carry out product/service updates for a defined period.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Product safety**	i. Users are provided with necessary information on the quality of the products and services (description, properties etc.). ii. Product and service is continuously updated for a defined period.

Table 13: Criterion – Product safety

5.10. Law enforcement declaration

In cases where users are faced with problems or believe that they have been harmed in their rights and freedoms, for example in their right to privacy, it is highly important to have the appropriate information and mechanisms in place, which would guide them in the process of

dealing with those harms via judiciary means. In order to ensure that, an ICT provider should clearly inform its users about two basic aspects:

(a) In cases where users believe they have been harmed, they should be informed *whom* they could hold accountable for a particular issue. This demands that a clear division of responsibilities exists so that users can easily determine, for instance in cases of a privacy-related issue, who is the data controller or processor;

(b) The other aspect relates to the question *where* they can initiate such processes. For that purpose, it should also be made clear whose national laws apply for a particular product or service.

TRUSTWORTHINESS ENHANCER	CRITERION	INDICATORS
Transparency Privacy Anti-discrimination Autonomy Respect Protection	**Law enforcement declaration**	i. Controllers and processors of the product/service are clearly determined. ii. Applicable national law for product/service is determined. iii. Users are informed that they can file a lawsuit at their place of residence.

Table 14: Criterion – Law enforcement declaration

5.11. Appropriate dispute resolution

The main aim of this criterion is to emphasize that apart from judiciary mechanisms there are also other possibilities to resolve issues and problems that may arise related to ICT products and services. Such example includes appropriate dispute resolution and applying alternative and non-judiciary mechanisms to problem-solving. These may often prove to be more user-focused, effective, not time-consuming, flexible and cost-effective. Moreover, they offer multiple-level solutions depending on the severity and complexity of the problem:

(a) Providing information about more common and less complex issues: This may come in the form of FAQ, which is easily accessible and understandable to users. This is considered to be the most basic level of problem-solving.

(b) In cases the provided FAQ do not fully address the concerns of users, there are other mechanisms users can resort to such as filling in a form, be advised by a contact person, call centre etc.

(c) For graver problems, there are mechanisms for professional dispute resolution, which may include but are not limited to informal mediative processes.

TRUSTWORTHINESS ENHANCER				CRITERION	INDICATORS
Transparency				**Appropriate dispute resolution**	i. Adequate mechanisms for problem solving beyond law enforcement and official judicial mechanisms. a. Necessary information is provided to assist in dealing with some problem (e.g. FAQ). b. If the information provided in a. does not help, further measures are provided, such as a form, contact person or centre that assist the user in solving the problem. c. If the problem cannot be solved by the measures provided in b., the possibility of professional alternative dispute resolution is provided, such as informal mediative processes.
Privacy					
Anti-discrimination					
Autonomy					

Respect					ii. Information is provided about where the user can exercise her rights. iii. Information is provided about against whom the user can exercise her rights.
Protection					

Table 15: Criterion – Appropriate dispute resolution

6. Recommendations

Based on the findings from the legal and ethical support study as well as stakeholder input a preliminary list of recommendations was compiled. The stakeholder input came from two sources. On the one hand, the Core Areas of trustworthiness and the first findings of D4.3 were presented and discussed at the TRUESSEC.eu Advisory Board Meeting in February 2018 in London. On the other hand, at end of June 2018 the University of Graz organised the International conference "In ICT We Trust 2018", which was also followed by a debate and workshop. Representatives from a number of EU projects took part in the conference. This set the ground for a fruitful discussion and exchange on the TRUESSEC.eu Criteria Catalogue but also on key issues relevant for the TRUESSEC.eu project and the other EU projects such as trustworthiness and ICT, the human factor in ICT, translation of social science and humanities expertise into technical and regulatory standards etc.

Some of the drafted recommendations can be seen as direct continuation of the Criteria Catalogue and the identified Core Areas, whereas others pertain to a much broader societal level and address issues such as digital divide, social inclusion, data ownership etc. This list will be further developed within WP7.

1)	Users should be given the possibility for an authentic assessment of and feedback on (a) a label and (b) the provider of the ICT product and service that is certified by that label.
2)	Users should be able to see the reviews and the provided feedback from other users when purchasing a product or using a service.

3)	Freedom of expression and of censorship should be respected.
4)	A label should support not only big and established companies but also start-ups.
5)	There should be a form or a check-list, which would enable to cross-check whether the specified criteria are fulfilled.
6)	Children protection and applying age limit to the use of certain ICT product and services should be taken into account.
7)	In order to encourage social inclusion and overcome the digital divide, appropriate measures should be taken, which would help disadvantaged groups to also make better use of these products and services.
8)	The question of data ownership should be part of discussions on ICT.
9)	Greater focus should be laid on digital education and raising awareness regarding ICT products and services as well as the impact these may have on users.
10)	Hate speech should be controlled but at the same time it ought to be ensured that cyberspace is a space where everyone can express their opinions and views.

7. Conclusion

With the increased presence of ICTs in our lives as well as the increased complexities and uncertainties that go hand in hand with that, the question of how trustworthy these technologies are becomes more and more relevant. Users need guarantees that the ICT products and services they use are in line with ethical and legal standards. This means that European values and fundamental rights are the basis for trustworthy technologies. Only in this way we can have a healthy information society with users who trust the products and services they purchase and use.

Within the TRUESSEC.eu project and as part of this report we have developed a **First draft Criteria Catalogue** for security and privacy features of ICT products and services and **recommendations** for the development of a European label for enhancing trust and security in Internet-based technologies and services. At this stage, the Criteria Catalogue entails mainly the input from two disciplines represented in the project, ethics and law. This First draft will pave the way for more interdisciplinary work, which will follow in WP7 where the input from the other three disciplines, sociology, business and technology, will be included as well.

These are the steps we took and the main findings we have formulated as part of this report:

1) Based on the support studies carried out in the first year of the project as well as based on some interdisciplinary work, we have agreed upon six **Core Areas**, which make up the basis of the TRUESSEC.eu Criteria Catalogue. These include: transparency, privacy, anti-discrimination, autonomy, respect and protection. The input we have provided in this report comes only from ethics and law, although we have also started to involve the other disciplines and partners.
2) The six Core Areas helped us and guided us in the search of legal and ethical **criteria** that may be used to evaluate the trustworthiness of ICT products and services. So far we have identified eleven criteria.
3) To each criterion we have assigned corresponding **indicators**, which should tell us to what degree a criterion is fulfilled. The list of criteria and indicators is not complete since with the fast pace of technological advancement it is likely to expect that the need may arise to include additional criteria. Nevertheless, the eleven criteria provided in the Criteria Catalogue can be considered as the fundamental ones.
4) We have also formulated **recommendations** to strengthen the role of fundamental rights and European values in the further development of ICT products and services.

The work that has been done as part of D4.3 will be further developed in WP7. It will mainly feed the development of the transdisciplinary Criteria Catalogue as well as the TRUESSEC.eu recommendations for trust-enhancing label.

8. References

BROWN, ALEXANDER. "A Theory of Legitimate Expectations", *Journal of Political Philosophy* vol. 25 no. 4 (2017): 435-460.

GIBELLO, VALENTIN. "TRUESSEC.eu - Deliverable D4.1. Support Study: Legal Analysis", 2017, published on https://truessec.eu/library.

BEIMROHR, Veronika. "Annex to Deliverable D4.1. Overview over the Legal ICT-Framework", 2017, published on https://truessec.eu/library.

Proposal for TRUst-Enhancing certified Solutions for SEcurity and protection of Citizens' rights in digital Europe.

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

STELZER, HARALD/ VELJANOVA, HRISTINA. "TRUESSEC.eu - Deliverable D4.2 Support Study: Ethical Issues", 2017, published on https://truessec.eu/library.