D6.1 Research Ethics

Authors: **Dutkiewicz Lidia, Miadzvetskaya Yuliya (CiTiP – KU Leuven)**

February 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481

TRUSTS Trusted Secure Data Sharing Space

D6.1 Research Ethics

Document Summary Information

Grant Agreement No	871481	Acronym	TRUSTS
Full Title	TRUSTS Trusted Secure Data Sharing Space		
Start Date	01/01/2020	Duration	36 months
Project URL	https://trusts-data.eu/		
Deliverable	D6.1		
Work Package	WP6		
Contractual due date	M14	26 February 2021	
Nature	Report	Dissemination Level	Public
Lead Beneficiary	KUL		
Responsible Author	Dutkiewicz Lidia, Miadzvetskaya Yuliya		
Contributions from	-		

Revision history (including peer reviewing & quality control)

Version	Issue Date	% Complete[1]	Changes	Contributor(s)
V0.1	20/11/2021	5%	Initial Deliverable Structure	KUL (Yuliya Miadzvetskaya)
V0.2	21/01/2021	90%	Internal submission for internal review (KUL)	KUL (Yuliya Miadzvetskaya, Lidia Dutkiewicz)
V0.3	19/02/2021	95%	Internal review (KUL)	KUL (Lidia Dutkiewicz)
V1	22/02/2021	100%	Submission to LUH for internal review	KUL (Yuliya Miadzvetskaya, Lidia Dutkiewicz)
v1.1	23.02.2021	100%	Internal review at LUH	LUH (Michael Fribus, Gerrit Rosam, Alina Brockob)

Disclaimer

[1] According to TRUSTS Quality Assurance Process:

1. to be declared

Copyright message

Table of Contents

List of Figures

List of Tables

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AI	Artificial Intelligence
c185	Convention 185
CAHAI	Ad hoc Committee on Artificial Intelligence
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPIA	Data Protection Impact Assessment
ECCRI	European Code of Conduct for Research Integrity
ECHR	The European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
GDPR	General Data Protection Regulation
HLEG	High-Level Expert Group
RRI	Responsible research and innovation framework
TEU	Treaty on the European Union
TFEU	Treaty on the functioning of the European Union
WP29	Working Party 29

1 Executive Summary

In this deliverable, we analyse the research ethics principles in order to address the legal and ethical issues arising from the research activities that will be conducted in the course of the TRUSTS project. Ethics is a primary concern for researchers. Ethics underlies European law and provides guidance when navigating the ambiguities of legal norms. Ethical standards provide guidelines and should be respected when researching and developing new solutions, which may fall in a yet unregulated area, such as AI. Ethics plays an important role when considering the appropriate course of action in conditions of uncertainty.

The development, testing and validation must comply with ethical principles to respect the individuals involved and to prevent harm. TRUSTS adheres to the ethics adopted throughout the European Union (EU) and embeds it in the planning, development, testing and implementation of its socio-technical solution. The scope of this report is to introduce the ethical landscape applicable for TRUSTS. We do it by, on the one hand, analysing relevant sources of ethics obligations such as the H2020 ethics code of conduct and, on the other hand, highlighting the areas of concern within the project such as the use of AI systems.

To that end, first, we discuss research ethics to provide an overview of the moral norms that researchers ought to respect when carrying out their activities. These include the EU Regulation No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon2020 - the Framework Programme for Research and Innovation (2014-2020)", the European Code of Conduct for Research Integrity, the Ethics in Social Science and Humanities drafted in 2018 by a panel of experts at the request of the European Commission (DG Research and Innovation), and the European Commission Decision C(2020)1862 of 25 March 2020.

Second, as TRUSTS aims at combining formal methods and reasoning techniques with inductive ones such as machine learning (ML), we discuss the ethical concerns around AI. We note that there are more than 116 “AI ethics” documents. All these documents however, reveal a common understanding on some generic principles including: respect for human autonomy, prevention of harm, fairness and explicability. To this end, we focus on the two documents: AI HLEG Guidelines on Trustworthy AI and the Recommendation of the Council on Artificial Intelligence by the OECD.

Third, the ethical foundations of data protection are presented. We offer an ‘helicopter view’ of the sources of law which must be complied with by the consortium in the development of the technology within the TRUSTS project. The legal framework susceptible of application to TRUSTS includes, inter alia, the international treaties such as the European Convention of Human Rights, the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108), the so-called Convention 108+ and the Budapest Convention. The European Convention of Human Rights recognizes the right to privacy as a fundamental human right. We then explain the set of regulations adopted by the EU in the area of privacy and data protection, which concretize this right to privacy. Such

regulations include both the primary EU law (the Treaties) and secondary law, such as the GDPR and ePrivacy Directive.

In Chapter 6 we offer a step-by-step explanation on the main data protection and ethics related concepts from the Background note relevant for the project lifecycle. These include, inter alia, ethical issues in using data (e.g. confidentiality, informed consent) and in managing and sharing data (e.g. initial and further processing, lawful basis).

Finally, we also attach relevant documents related to the processing of personal data within the project activities.

We consider this ethics deliverable as a consistent set of measures aimed at ensuring compliance with ethics requirements within the TRUSTS project. Compliance with ethics and legal requirements is considered as a continued effort by the partners to be maintained throughout the project.

2 Introduction

2.1 Mapping Projects' Outputs

This report outlines the result of the ethical and legal analysis of TRUSTS. The project aims at the development and testing of a federated data marketplace. The lack of trusted and secure platforms and privacy-aware analytics methods for secure sharing of personal data and proprietary/commercial/industrial data hampers the creation of a data market and data economy by limiting data sharing mostly to open data. This trend will continue if different technical standards, quality levels, and legal aspects are allowed to diverge uncontrollably.

TRUSTS will ensure trust in the concept of data markets as a whole via its focus on developing a platform based on the experience of two large national projects, while allowing the integration and adoption of future platforms. The TRUSTS platform will act independently and as a platform federator, while investigating the legal and ethical aspects that apply on the entire data valorization chain, from data providers to consumers, i.e. it will:

- ✔ Set up a fully operational and GDPR-compliant European Data Marketplace for personal related data and non-personal related data targeting both personal and industrial use by leveraging existing data marketplaces (International Data Space and Data Market Austria) and enriching them with new functionalities and services.

- ✔ Demonstrate and realise the potential of the TRUSTS Platform in 3 use cases targeting the industry sectors of corporate business data, specifically in the financial and telecom operator industries while ensuring it is supported by viable, compliant and impactful governance, legal and business model.

2.2 Deliverable Overview and Report Structure

The scope of this report is limited to international and EU law. National legislation is not taken into consideration at this stage of the project. The reason is that partners are spread across a number of jurisdictions for which an extensive analysis would be needed, which is beyond the scope and purpose of this document. It is recommended that, should legal and ethical questions arise concerning national regulations, partners address such inquiries to their internal legal departments. In addition, it is worth noting that this report, which is the result of the work performed under task 6.1, is designed to provide an overview of the ethical and legal framework that might apply to the activities of the consortium. The practical requirements of some of those principles were described in WP9 deliverables and will be further developed in D6.3 which deals with legal requirements for TRUSTS' platform development and later on also in deliverable D6.4, which will present the results of the mapping and analysis and provide recommendations at the end of the lifespan of the TRUSTS project.

The ethical and legal framework identified as relevant in this report have been chosen based on the scope of the TRUSTS-project, focusing on aspects of data protection and privacy law as well as cybersecurity applicable to the project.

The aim of this report is threefold:

- To outline the ethical principles that ought to drive research activities within the EU. These principles cover areas such as privacy, data protection and the use of AI and should be considered by the partners involved in activities that might have an effect on them;
- To flesh out the international legal framework that deals with the areas in which TRUSTS operates;
- To describe the EU sources of law that are applicable to the activities of the project.

The structure of this report is as follows:

- Chapter 3 provides background on how personal data are processed in the TRUSTS project;
- Chapter 4 elaborates on ethical norms applicable to research activities. It also provides guidelines on ethical use of artificial intelligence (AI) and machine learning (ML) systems. Finally, the ethical foundations of data protection will be presented;
- Chapter 5 describes the applicable legal framework and the core principles behind data protection. This includes international treaties and EU primary and secondary legislation;
- Chapter 6 provides a step-by-step explanation of the data protection obligations.

In Annex I we attach a questionnaire to partners - Ethics requirements with respect to personal data. Annex II and Annex III contain respectively a template of informed consent (data processing) and a consent form template (questionnaires, workshops, focus groups).

3 Background

During the research activities and the rollout of the project, personal information will be inevitably processed. Personal data within the TRUSTS project are processed pursuing a legitimate interest of the consortium. This means we have a contractual obligation to undertake a number of research activities. Such contractual obligations are found in the Grant Agreement No 871481 (lasting 3 years until 31 December 2022) that TRUSTS Consortium signed with the European Commission (REA Agency). Further legal rules relevant for our research activities are substantiated in Article 89(1)[2] of the GDPR and the European Union Regulation No 1291/2013 of 11 December 2013 Establishing Horizon2020 - The Framework Programme For Research And Innovation (2014-2020). In Deliverable 'D9.10 POPD - Requirement No. 16' submitted on 30 June 2020 we have provided a detailed analysis on processing personal data for research purposes.

- According to the GDPR (Article 4), 'controller' "*means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*; In substance, the controller is the person or entity which leads the personal data processing operation by determining purposes and means for the processing. In TRUSTS, processing operations are handled by different partners. However, supervision over such operations and the determination of purposes and means are dealt with by the responsible partners in close coordination with the entity responsible for the project (i.e., project coordinator). Below are the contact points of the project coordinator, should you have any query regarding the way personal data is processed: Alexandra Garatzogianni - H2020 Coordinator of TRUSTS Trusted Secure Data Sharing Space, Senior Project Manager, Leibniz University of Hannover, L3S Research Center & Head of Tech Transfer, EU-Project Coordination & Management, Leibniz Information Center for Science and Technology, University Library.

Since TRUSTS is a research project, we are conducting a number of pilot testing:

[2] Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

- Use case 1: The AML Services that will be used through the TRUSTS Platform by the providers FNET & InBestMe (or other Financial Institutions). As part of this project, we will leverage the power of the TRUSTS Platform in view of securely sharing data between organisations, applying smart big data analytics for AML compliance purposes as well as fairly trading the resulting data to end-users such as FIs, internal / external auditors, fiduciaries, audit firms, etc.
- Use case 2: The purpose is to verify that TRUSTS services can be used to advance current marketing activities extending towards enabling collaboration between different enterprises in a GDPR complaint manner.
- Use case 3: Automation of debt management: the data acquisition to improve customer support services use case. The TRUSTS Data Marketplace vision is to create an out-of-the-box analytics solution for the anonymization and visualization of Big Financial Data, specifically to advance new ways of human-computer interaction currently in their infancy, e.g. chatbots that can act as automated assistants to allow customers to converse about the management of their debt at their own pace and with a personalized experience, through the integration of Big Data.

Some information on the policy of the project and about the ways personal data are processed

However, processing personal information pursuing research interests implies that a number of safeguards and proactive initiatives are taken in order to protect your privacy rights. In order to do so, TRUSTS project partners begin all processing of personal data by following these principles:

- **Fairness and lawfulness**. Personal data are processed fairly and for the purposes for which they were collected initially. Moreover, personal data processing operations are assessed against their legality by the project coordinator.
- **Security of processing**. Personal data processing operations are conducted following the available security measures, both technical and organizational. As an example, access control and authentication-based environments are applied to the access to data-sets containing personal data, and the need-to-know principle is implemented in the vetting of any researcher involved in TRUSTS personal data processing operation.
- **Minimization**. Collection and processing of personal data, including during the technology testing and the data storage, follow the principle of data minimization. This means, for example, collecting your data in a way that only the strictly necessary amount of it is processed. Furthermore, the testing of TRUSTS technologies will be conducted only in circumscribed perimeters, and whenever personal details will be needed, pseudonymization will be sought.
- **Data retention period**. If immediate deletion will not occur, that means we have a legal obligation and/or a research purpose to archive the data either for contractual reasons or for scientific research finalities. If required, we may retain the information for a year after its termination. By then, personal data will be deleted. We will apply data anonymization and minimization techniques in order to minimize any risk of confidentiality breach or unintentional data breach.

- **Third-party non-disclosure**. No personal data will be disclosed to any third-party (i.e. non-consortium entities) unless there is an explicit authorization to do so by the interested individual.
- **Use-case-based access**. Personal data will remain within the consortium domain. Furthermore, personal data will only be accessed by the partners with an involvement in the use-case an individual is asked to participate in. If the partner does not have any interest or involvement in a use case, personal data processed therein will not be disclosed to them, in accordance to the need-to-know principle.
- **Long-term identification is not an aim**. It is not in the purposes of this project to retain personal data for long periods and to aggregate such data so as to identify you. When personal data are processed for research finalities, such sets will mostly be operated for the duration of the testing and immediately deleted afterwards, unless otherwise indicated.
- **Accuracy**. TRUSTS project regularly reviews datasets where personal data are stored in order to ensure the accuracy and reliability of the information therein. Systems to update the information are in place to ensure both security and controlled access to datasets.

If a data subject believes that any of its personal data are processed by TRUSTS, it is entitled to request the controller to undertake the following actions:

- **Right to access**. Data subjects are entitled to request information regarding personal data, including purposes, categories of information, recipients, retention, source of collection, transfer to third-countries (non-EU Member States). Moreover, the data subject is entitled to receive a copy of such data.
- **Erasure or rectification**. Data subjects may request at any time for their personal data to be amended, updated or erased by the controller.
- **Restriction of processing**. Data subjects have the right to request that their data are suspended from being processed, anytime the data results to be inaccurate or unlawfully or unnecessarily processed.
- **Object**. Data subjects have the right to object to the processing of their personal data, unless the processing is conducted on public interest grounds and pursuant to Article 89(1).
- **Automated decision-making or profiling**. Data subjects have the right not to be subjects to automated decision-making processes (including profiling) which substantiates in legal consequences for him or her.

- **Lodge a complaint** with a supervisory authority.

How we embed privacy within the consortium

TRUSTS project values the respect for privacy and data protection as both a legal requirement and an ethical standard. For this reason, we indicate below the periodical actions and initiatives we undertake in order to frequently review the way the project observes and respects privacy standards.

1. Respect for GDPR and its obligations in the scientific research domain. The main legal act we rely upon for complying with privacy and data protection rights is the GDPR. In this respect, we continuously assess our activities, particularly if or when involving personal data processing operations for scientific research purposes, against the rights of the individuals and our legal obligations enshrined in the GDPR.

2. Accountability. We maintain and regularly update internal policies enabling the consortium to keep records and documentation of the relevant personal data processing operations. These actions include the assessment of the risks that during our research may occur to the rights and freedoms of individuals. Such processes aim at identifying mitigation measures and enabling safeguards against privacy violation, and are recorded in the so-called DPIA (data protection impact assessment).

3. Awareness raising. We regularly undertake activities aimed at informing our consortium partners about the data protection obligations and standards that we abide to. Initiatives are performed on a periodical basis and include webinars, presentations and ad-hoc sessions on privacy, data protection and the respect for fundamental rights in research activities. Privacy sessions are organized in the course of every face-to-face general assemblies organized by the consortium.

4. Ethical standards. As said above, we do not only regard the protection of personal data and privacy as a legal requirement to meet. TRUSTS project considers personal data protection obligations as an ethical standard of best practice. For this reason, the consortium implements and assesses privacy beyond what imposed by law and as a by-design principle, including in the development of any technology and its integration within use-case scenarios.

5. Further research guidelines. TRUSTS project makes extensive use as a benchmark and as a code of conduct of further ethical guidelines issued by the European Commission on responsible research. Such manuals inform researchers and projects funded under the Horizon2020 and similar EU funding programs about the best practices to be adopted when the research involves the processing of personal data.

4 Ethics

4.1 Overview

Ethics is a primary concern for the EU. It underlies European law and provides guidance when navigating the ambiguities of legal norms. Ethical standards provide guidelines and should be respected when researching and developing new solutions, which may fall in an unregulated area. This might prevent undesired outcomes and will promote the goals of preventing harm and enable human flourishment.

The development, testing and validation must comply with ethical principles to respect the individuals involved, and to prevent harm. TRUSTS adheres to the ethics adopted throughout the EU and embeds it in the planning, development, testing and implementation of its socio-technical solution. The scope of this section is to introduce the moral landscape of TRUSTS by, on the one hand, analysing relevant sources of moral obligations such as the H2020 ethics code of conduct[3] and, on the other hand, highlight the areas of concern within the project such as the use of artificial intelligence techniques.

This section is structured as follows. First, research ethics will be discussed to provide an overview of the moral norms that researchers ought to respect when carrying out their activities. Second, the issues of AI ethics will be discussed. TRUSTS aims at integrating both facets of AI by combining formal methods and reasoning techniques with inductive ones such as machine learning (ML). Therefore, state of the art AI tools and methods will be developed by the technical partners. This is why the ethical concerns around AI will be broadly discussed to inform the consortium. Finally, the ethical foundations of data protection will be presented. While it is true that moral obligations in this area are often enshrined in data protection laws, the spirit and objectives of this area are found by examining the moral basis of the law. Ethics plays an important role when considering the appropriate course of action in conditions of uncertainty.

4.2 Research Ethics

The first relevant ethical aspect concerns research ethics. Throughout the development of TRUSTS particular attention shall be devoted to uphold fundamental norms of ethical research. This section introduces the sources of the relevant norms and summarizes the principles that should be at the core of research activities carried within the EU.

Under Article 19 of the Regulation 1290/2013[4], all research and innovation activities of Horizon2020 projects must comply with ethical principles. This section examines the principles that are relevant in the context of the research activities envisioned in the proposal, e.g. surveys. Ethical principles are, by nature, broad and comprehensive so that a certain overlap with other sections of this report is expected.

When examining the ethics of TRUSTS, it is crucial to start from the sources where applicable ethical principles can be found. On this basis, this section examines three documents. Namely, the European Code of Conduct for Research Integrity[5] (henceforth also, ECCRI), the Ethics in Social Science and Humanities drafted in 2018 by a panel of experts at the request of the European Commission (DG

[3] Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf

[4] Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in "Horizon2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006, OJ L 347, 20.12.2013, p. 81.

[5] Available at: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf

Research and Innovation)[6], and the European Commission Decision C(2020)1862 of 25 March 2020[7]. The next paragraphs examine each one in order.

First, Article 1 of the ECCRI states four ethical principles to which the consortium ought to adhere as they lie at the core of ethical research. These are:

- Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources;
- Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way;
- Respect for colleagues, research participants, society, ecosystems, cultural heritage and their environment;
- Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring and for its wider impacts.

The second document concerns the Ethics in Social Science and Humanities, which contains important principles to inspire the activities of the TRUSTS partners. For example, the proposed use-cases of the project might require the participation of vulnerable subjects, such as participants in a dependent relationship with one of the partners involved in the pilot. While a more granular exposition of the relevant ethical issues is performed in WP9 requirements, it is necessary to describe the ethical principles enumerated in the aforementioned document that might be relevant for the activities of the TRUSTS consortium.

Amongst the overarching ethical principles stated in the context of SSH the most salient are the following:

- Respecting human dignity and integrity;
- Ensuing honesty and transparency towards research subjects;
- Respecting individual autonomy and obtain free and informed consent;
- Protecting vulnerable individuals;
- Ensuring privacy and confidentiality.

The above mentioned principles ought to inform all of the activities carried out in TRUSTS. Of course, many of these principles are also part of the legal framework applicable to the project, such as privacy.

Consent of the subjects involved in the project is also crucial to ensure the respect for the highest ethical standards. It plays a foundational role in various aspects of research, from the recruitment of the participants to the legal basis to process personal data. Most of the literature on consent stems from clinical research where its role is crucial, however, this requirement has also been extended to other areas that are touched upon by the project, such as data protection and the participation in other data gathering activities such as surveys. Accordingly, the basic elements of consent that are relevant for TRUSTS can be summarized as follows:

[6]Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_ethics-soc-science-humanities_en.pdf

[7] Available at: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-swfs_en.pdf

- Freedom; subjects must be in a situation in which they do not fear undesirable consequences if they refuse to participate in the research. This is because no real free choice can be made when external pressure weighs on participants. This aspect is critical when subjects may be in a subordinate position with respect to the persons or entity promoting the research;
- Specificity; subjects must be able to precisely discern the research activities they are consenting to. This includes elements such as the purpose of the research, the expected duration, the description of the procedures and research activities and so on.
- Informed; subject must be informed on the possible implications of the research including expected benefits, risks and the strategies to mitigate them. Concerning data protection, informed consent is ensured by describing the purpose, duration, and policies to respect data protection regulations.

Lastly, the Decision C(2020)1862 establishes part of the work programme for Horizon2020 concerning science with and for society. This document contains an important reference to the responsible research and innovation framework (RRI) that cuts across all the research activities carried out within Horizon 2020. The Commission regards RRI as a "process for better aligning research and innovation with the values, needs and expectations of society"[8]. The RRI framework aims to avoid irresponsible innovation characterised – for example – in four types:

- Technology push (which occurs when technological innovations are pushed to market without prior consultation or other suitable deliberative mechanism);
- Negligence of fundamental ethical principles;
- Policy pulls (which occurs when technologies are pulled from research for political reasons);
- Lack of precautionary measures and technology foresight[9].

These instances prevent innovation activities to be responsible and to serve the European societies. Notably, some of the strategies to promote RRI can be summarized as follows:

- Use of technology assessment and technology oversight;
- Application of the precautionary principle;
- Multi-stakeholderism;
- Codes of conducts;
- Standards, certifications and self-regulation;
- Ethics by-design approach**.**

4.3 Artificial Intelligence Ethics

TRUSTS aims at providing better analytics and assessment. This entails that machine learning models and formal reasoning techniques will be tested in the upcoming months. On this basis it seems appropriate to devote a section on the ethics of artificial intelligence. Thus, this section first examines if the tools

[8] Supra p. 8.

[9] Von Schomberg, Rene, "A vision of responsible research and innovation." Responsible innovation: Managing the responsible emergence of science and innovation in society (2013): page 51-74.

developed by the consortium are likely to fall under the definition of artificial intelligence and, second, provides an overview of the growing subfield of applied ethics concerned with AI.

Although there is no universally accepted binding AI definition, the Communication from the Commission on Artificial Intelligence for Europe (25.04.2018 COM(2018) 237) states that: *"Artificial Intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.*

AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistant, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or internet of Things applications)[10]*."*

The above definition was subsequently expanded by the high-level expert group on artificial intelligence assembled by the Commission (AI HLEG) in the Ethics Guidelines for Trustworthy AI: *"Artificial Intelligence (AI) systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge or processing the information, derived from the data and deciding the best action(s) to achieve a given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behavior by analysing how their environment is affected by their previous actions […]*[11]*."*

The AI HLEG goes on to enumerate some of the techniques that fall under their definition of AI in which machine learning and formal methods for knowledge representation and reasoning are included. The rapid increase in AI applications has spurred numerous contributions concerned with the ethical requirement for its good use. In recent years, private companies, academic and public-sector organisations have issued principles, guidelines and other soft law instruments for the ethical use of AI. As noted by the Ad hoc Committee on Artificial Intelligence (CAHAI) Feasibility Study[12], there are more than 116 documents on "ethical AI", primarily developed in Europe, North America and Asia.[13] All these documents reveal a common understanding on some generic principles. However, when it comes to giving practical guidance, they tend to sharply disagree over the details. This issue will need to be addressed by policy makers.

This section considers two prominent documents. The AI HLEG's Ethics Guidelines for trustworthy AI and the Recommendation of the Council on Artificial Intelligence by the OECD (OECD/LEGAL/0449[14]). This is because, as shown by an important survey of all the ethics guidelines on AI[15], most documents overlap in

[10] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe COM/2018/237 final.

[11] Available at: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[12] Ad hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, CAHAI(2020)23, available at: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

[13] Ibid., p.20.

[14] https://oecd.ai/assets/files/OECD-LEGAL-0449-en.pdf

[15] Floridi, Luciano, Josh Cowls, Monica Beltrametti, Raja Chatila, Patrice Chazerand, Virginia Dignum, Christoph Luetge et al. "AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations." Minds and Machines 28, no. 4 (2018): 689-707.

their suggested principles. The next paragraphs expose the high-level core principles of the ethical AI that ought to inspire the consortium.

The first document addresses the need for an ethical AI as one of the three components necessary to build a trustworthy AI, the other two being lawful and robust. At the onset, the AI HLEG Guidelines describe the need for AI systems to be human-centric, to serve humanity and with the goal to improve human welfare and freedom. This approach entails maximising the positive outcomes of AI systems and minimising their risks in order to prevent harm. In line with the expert group guidelines, the consortium is committed to these goals as shown by the tasks devoted to the ethical assessment of the sociotechnical solution. The ethical manager should be involved when evaluating distinct architectural choices of the systems which might all be capable of achieving the target result to select the least likely to have a negative ethical impact.

The AI HLEG grounds ethical AI on the respect of fundamental rights enshrined in international human rights law, the EU treaties and the EU charter. These sources of law will be analysed in more detail below. That said, the root of the four ethical principles is human dignity reflected by the human-centric approach adopted by the expert group. These principles considered as ethical imperatives are:

- Respect for human autonomy;

In practice, the principle of respect for human autonomy means that humans interacting with AI systems must be able to keep full and effective self determination. AI systems should not unjustifiably subordinate, coerce, deceive, manipulate, condition or herd humans.

- Prevention of harm;

The prevention of harm principle means that AI systems and the environments in which they operate must be safe and secure. They must be technically robust and should not cause or exacerbate adverse impacts due to asymmetries of power or information, such as between businesses and consumers or governments and citizens. Preventing harm also entails consideration of the natural environment and all living beings.

- Fairness;

Fariness implies a commitment to: ensuring equal and just distribution of both benefits and costs, and ensuring that individuals and groups are free from unfair bias, discrimination and stigmatisation. The procedural dimension of fairness also entails the ability to contest and seek effective redress against decisions made by AI systems.

- Explicability;

Explicability means that AI processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected.

The Council of the OECD echoes and expands the principles stated by the AI HLEG Guidelines. It also aims to establish a paradigm for trustworthy AI through ethical, legal and technical guarantees. The relevant principles established by the OECD are the following:

- Inclusive growth, sustainable development and well-being;
- Human-centred values and fairness;
- Transparency and explainability;
- Robustness, security and safety; and
- Accountability.

The scope of these principles is broader than that of the AI HLEG for reasons related to the wider scope of the OECD's mandate. However, in striving for the highest levels of ethical acceptability of AI systems they ought to be taken into consideration by the partners.

4.4 Data Protection Ethics

Data protection is a fundamental ethical issue in Europe, it is also a fundamental human right and respect thereof is required by law. However, data protection ethics goes beyond compliance with data protection legislations. It is a broader concept intimately linked to human dignity and autonomy. It is possible and in some cases desirable from an ethics point of view, for example, to go beyond complying with data protection laws and to develop solutions that guarantee more protection than what is strictly legally required. While most of the normative content of data protection ethics is enshrined in legal obligations, such as the GDPR, ethical considerations become poignant when interpretative issues arise regarding so-called legal grey areas, enforcement activities or in the absence of explicit legal guidance. It is not always clear-cut what the differences are between ethics and legal requirements. This will be discussed under upcoming deliverables, and in particular D3.1. On this basis, it appears necessary to discuss the moral foundations of data protection as identified by a panel of experts at the request of the Commission (DG Research and Innovation) in 2018[16].

Ethical considerations on data protection apply when personal data is processed. It is foreseen that personal data will be processed at least for parts of the development of the TRUSTS solution. What kind of personal data and to what extent it will be processed will become clear as the project develops. However, it is necessary to describe the core principle behind data protection ethics already at this stage. Human dignity and autonomy are the central principles.

5 Legal Framework

5.1 Overview

The following sections of this report concern the legal framework susceptible of application to TRUSTS. It provides an 'helicopter view' of the sources of law which must be complied with by the consortium in

[16] Ethics and data protection, available at: https://ec.europa.eu/info/sites/info/files/5._h2020_ethics_and_data_protection_0.pdf

the development of the technology necessary to achieve the aim of the project and during the piloting phase.

5.2 International Treaties

The partners of TRUSTS are established in jurisdictions that are subject to a number of legal obligations found in international treaties. International treaties are applicable foremost to ratifying states and sets obligations for these states to ensure the rights enshrined in the treaties and conventions. This is also the case for the conventions presented below. However, since TRUSTS is established in ratifying states, the conventions are relevant sources to take into account, as they entail the principles laying the grounds for EU and national legislation. The ensuing sections provide an overview of the international legal instruments that might be relevant for TRUSTS.

5.2.1 The European Convention on Human Rights (ECHR)

The ECHR[17] is an international treaty ratified by all Member States of the European Union and, which is relevant for the consortium, Israel. The ECHR protects fundamental human rights and liberties. Amongst its provisions, of particular relevance for TRUSTS is Art. 8, that covers the right to respect for private and family life. It states:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Art. 8 establishes the basic form of the right to privacy. It should be noted that the concept of private life is broad and includes the activities planned by the consortium, inter alia, the collecting and processing of personal data for research purposes and the protection of platforms (intermediaries) from cyber and physical threats.

However, the ECHR does not create obligations for private legal persons, rather it is directed at incentivizing states to establish the appropriate legal instruments to ensure the protection of these rights. That being said, natural and legal persons can bring states before the European Court of Human Rights (ECtHR) for violations of the ECHR by not ensuring an adequate level of protection. In the context of Art. 8, it entails that any interference with the right to privacy must be in accordance with the law. In addition, the interference shall be balanced with competing values and objectives of democratic societies. The normative content of Art. 8 is both negative – abstain from interference – and positive, that is signatories must implement appropriate measures to ensure that Art. 8 is respected in their territories. Of particular relevance is the necessity test which is essential to justify violations of Art. 8, in

[17] Council of Europe, European Convention on Human Rights, 1950 as amended, available at: https://www.echr.coe.int/Documents/Convention_ENG.pdf

the jurisprudence of the ECtHR *"the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"*[18]. Thus, necessity implies proportionality which – as will be discussed below – is also a requirement under EU law.

In the context of TRUSTS, the direct application of the ECHR appears to be limited, due to the comprehensive set of regulations adopted by the EU in the area of privacy and data protection, which concretises the right to privacy.

5.2.2 The Council of Europe's Convention 108

The Convention for the protection of individuals with regard to automatic processing of personal data[19] (also known as Convention 108) is the only instrument of international law concerning solely the protection of personal data.

Adopted in 1981, the Convention acts as the cornerstone of several data protection legal frameworks. This instrument imposes obligations for the signatories to implement appropriate safeguards into national law. The convention is not directly applicable to TRUSTS, but is binding for its ratifying parties. The states where the partners of TRUSTS are established are signatories of the Convention 108 and therefore, the principles laid down in the Convention are relevant to discuss. The basic principles of data protections established by the Convention 108 are worth illustrating. These principles, found in Art. 5, are the following:

- Lawful and fair processing;
- Purpose limitation;
- Data quality and accuracy;

It is evident, *prima facie*, how the aforementioned principles laid the foundations for modern data protection instruments. In addition, the Convention 108 introduce the distinction between personal and sensitive data. The former are qualified according to Art. 6 as "*personal data revealing racial origin, political opinions or religious or other beliefs as well as personal data concerning health or sexual life*".

The Convention also provided the first rights for data subjects to be established by its signatories. These rights – as stated in Art. 8 - are:

- Right to information;
- Right to rectification or erasure.

The Convention 108 has an established role in the jurisprudence of the European Court of Human Rights ("ECtHR"). The judges in Strasbourg often refer to the Convention 108 as an interpretative tool in assessing the scope of the aforementioned Art. 8 ECHR.

[18] ECtHR, *Leander v. Sweden,* No9248/81, 26 March 1987, para. 58.

[19] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 1981.

Another important aspect of data protection was first addressed by the Convention, namely the international transfer of personal data. Chapter III deals with the transborder flow of personal data, it introduced the basic principle for the legitimate cross-border transfer of data, i.e. equivalent protection. This principle is still prominent in the instruments governing transnational data flow as will be discussed further in this report.

The Council of Europe ("CoE") has updated the Convention to reflect the technological changes and the new methods of processing personal data, which have occurred since its inception. The modernization process resulted in an updated version of the text, namely the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, also known as the Convention 108+. Without intervening on the principles at the core of the original Convention, this revision aims at extending its application to a wider range of players to prevent forum shopping by data controllers (i.e. the practice of relocating a business entity to a different jurisdiction with less stringent legal requirements).

Relevant novelties of the Convention 108+ are the following. First, an updated definition of the category of special personal data is provided in Art. 6, with the notable inclusion of biometric data. Second, Art. 9 introduces the right of data subjects *"not to be subject to a decision significantly affecting him or her based solely on automated processing without having his or her view taken into consideration"*. This translates into an obligation for providers of technologies like big data analysis tools or machine learning/artificial intelligence algorithms to lay down transparent and explainable processes within their design activities[20]. This provision appears *prima facie* relevant for TRUSTS, however, a similar norm is found within the GDPR, which is, as an EU secondary legislation, directly applicable to the consortium of TRUSTS.

5.2.3 The Budapest Convention

TRUSTS aims at establishing a data market place that is resilient to cyber and physical threats. It is likely that parts of the set of cyber threats qualify as cybercrimes under international law, thus a brief overview of the Budapest Convention[21], or Convention 185 (henceforth, also c185) is in order. Adopted in 2001 by Council of Europe ("CoE"), c185 established an international standard for the criminalization of cyber-related offences. C185 has been ratified by 65 states, and it applies to all the states in which the members of the consortium are established.

The main effect of c185 is requiring participating jurisdictions to amend their criminal statues pursuant to the content of c185. More precisely, c185 targets the conducts directed to compromise the CIA-triad, that is data and network Confidentiality, Integrity and Availability. In addition, it enumerates a number of criminal offenses that belong to the following categories:

- Computer-related crimes;

[20] Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' [2016] arXiv.org; Ithaca <https://search.proquest.com/docview/2074006289?rfr_id=info%3Axri%2Fsid%3Aprimo> accessed 20 May 2019.
[21] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

- Computer-assisted crimes;
- Computer-environment crimes.

Lastly, c185 introduces several mechanisms for the international cooperation of enforcement bodies on electronic data and related evidence exchange[22]. It is also important to note that the CoE has started a public consultation to draft an additional protocol to c185 on the issue of electronic exchange of evidence.

While c185 is not directly applicable to the partners or to the project as a whole, it might provide a starting point to map some of the existing threats to online intermediaries by cataloguing the conducts classified as cybercrimes that are likely to affect online intermediaries.

5.3 Primary EU Legislation

This section introduces the primary legislation of the EU applicable to TRUSTS by providing an overview of the relevant legal instruments and their provisions. The following sources of law will be discussed in the ensuing paragraphs: the Charter of Fundamental Rights of the European Union ("the Charter"), the Treaty on the European Union ("TEU"), and the Treaty on the Functioning of the European Union ("TFEU").

5.3.1 The Charter of Fundamental Rights of the European Union (Charter)

Entered into force in 2009, the Charter of Fundamental Rights of the European Union[23] is a synthesis of the Member States' constitutional traditions. The importance of the Charter is twofold. On one hand, it lays the basis for guidance for the ethical values established within the EU. In this capacity, it also drives moral actions of institutions and Member States alike and provides guidance when new technologies are developed in legal grey areas. On the other hand, the Charter is legally binding for all EU institutions and all Member States of the EU since 2009 and a primary source of EU law. As such it establishes the fundamental rights of EU citizens and it lays the basis for all legislation and actions by the EU and its Member States.

The relevant provisions for TRUSTS are Article 7 and Article 8. The former is rubricated "*respect for private and family life"*, the latter *"right to personal data protection"*. Article 7 establishes the right to privacy of citizens in several areas, from private life to communications. For the purpose of this deliverable it is useful to state the full text of the aforementioned provisions.

Article 7 reads:

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8:

[22]Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Crime and society series). Cambridge: Polity press.

[23] Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 389.

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

These provisions establish the fundamental requirements for the processing of personal data within the EU. These basic principles of EU law find application in secondary sources of law, such as the ePrivacy Directive[24] and the GDPR, which will be discussed later in this report. Another relevant provision of the Charter is Article 52(1), which sets the scope of the fundamental rights. Hence, it provides the legal basis and justifications for the limitations of such rights within the European legal order. In this context, this norm grounds the limitations on the right to privacy and data protection.

It reads:

"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality limitations may be made only if they are necessary and genuinely meet the objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

On this basis, limitations on the exercise of the rights and freedoms recognised by the Charter are valid if they:

- Are provided by law;
- Respect the essence of the right;
- Are proportionate and necessary;
- Meet the objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

The scope of the rights is thus similar to the ECHR. The reference to the essence of the rights and freedoms is significant. It means that limitations that are so extensive as to devoid a fundamental right of its basic content are unlawful[25]. Note that, if the essence of a right is not respected it is irrelevant if the limitations meet the requirements concerning the general interest or are necessary to protect other rights or freedoms. Furthermore, the respect for the essence of rights enables a distinct interpretative lens to assess the validity of possible limitations, thereby reinforcing the importance of the Charter from the ethics perspective as it has been highlighted in the first part of this report.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications, OJ L 201, 31.7.2002, p. 37.
[25] Giakoumopoulos, Christos, G. Buttarelli, and M. O'Flaherty, "Handbook on European data protection law." (2018). p. 43.

5.3.2 The Treaty on the European Union and the Treaty on the Functioning of the European Union

The two Treaties[26] lay the foundation of EU primary law together with the Charter. In their consolidated version of 2009, they are also known as Lisbon Treaties.[27] They establish the governance structure of the EU, its agencies, fundamental principles, the legal basis for all EU legislation and underlying policy objectives. In the context of TRUSTS several provisions are relevant.

Starting from the TFEU, Article 16 restates data protection as a fundamental right of the EU, and lays the legal basis for legislation in the sphere of data protection. More precisely it reads:

"1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."

It also establishes the competency of the European Parliament and the Council to legislate on matters related to the processing of personal data. This is a landmark development in data protection law, because before the legal basis for data protection instruments – such as the Data Protection Directive – was the internal market[28]. Moreover, Art. 16 TFEU also restates that the compliance with data processing rules shall be subject to control of an independent authority. The content of this Article corresponds to that of the sources of international law examined above.

While the sources of secondary EU law establish the framework for the protection of personal data, Article 16 of TFEU directly protects individuals, even in the absence of secondary legislation. This is consistent with other fundamental rights enshrined in the TFEU such as the freedom of movement.

Article 16 of the TFEU refers to Article 39 of the TEU, which is also worth mentioning in the context of TRUSTS. The TEU establishes the EU, its central institutions (and respective governance structure) and the founding rules on the values of the EU as well as e.g. external, foreign and security policy. In its present form, Article 39 states that the Council shall – in derogation of Article 16(2) TFEU – establish the rules relating to the protection of personal data when carrying out activities relating to foreign and security policy. In addition, the competency of the Council concerning the free movement of personal data is also established, as concerns foreign and security policy.

It can be anticipated that the practical relevance of these provisions for TRUSTS is limited. Most of the applicable legal framework to the activities planned by the members of the consortium are covered by secondary EU sources to which this report now turns. However, in cases of legal uncertainty, guidance and interpretation shall be in accordance with the implementation of the sources of primary EU law and international treaties and conventions.

[26] Consolidated version of the Treaty on European Union, OJ C 202 7.6.2016, p. 13 and Consolidated version of the Treaty on the Functioning of the European Union, OJ C 202 7.6.2016, p. 47.
[27] The 2009 consolidated version of the Treaties were ratified under the Lisbon Treaty.
[28] See supra, note 13.

5.4 Secondary EU Legislation

5.4.1 Preliminary remarks

The secondary legislation of the EU consists of regulations, directives and decisions. It operates under the principles and objectives enshrined in the EU Treaties on the basis of the principle of conferral. The next sections deal with the sources of secondary EU law that may apply to TRUSTS, with the goal to provide an overview of the most important norms and principles; a more granular discussion of the legal requirements of TRUSTS was included in D6.2 and will be further developed in D6.1.

5.4.2 The General Data Protection Regulation

5.4.2.1 Background and scope of the GDPR

On the basis of the above mentioned Article 16(2) TFEU, the European Parliament the European Council adopted the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (known as the General Data Protection Regulation or GDPR) in 2016. The GDPR repeals the Data Protection Directive (Directive 95/46/EC) and is designed to regulate the processing of personal data in a variety of contexts. It is important to note that the GDPR is a Regulation whilst the previous instrument was a Directive. The former is directly applicable within the EU, whereas, the latter requires the transposition by Member States into their national legal systems. That being said, the GDPR allows some level of discretion for Member States in certain cases, such as the age requirement necessary for the applicability of the discipline on child's consent[29]. This being said, it should also be noted, that the GDPR is directly applicable to TRUSTS and therefore applies to all the partners and actions of TRUSTS.

Against this background, the ensuing paragraphs describe the scope and main features of the GDPR from a general perspective. Doctrinal debates and interpretative doubts are purposefully omitted due to the nature of this report. Similarly, the specific requirements of data protection concerning the sociotechnical solutions developed by the consortium are not within the scope of this document.

The GDPR applies when personal data is processed "*wholly or partly by automated means*" and when the processing with other than automated means forms "*part of a filling system*" or it is intended to[30]. On this basis the notions of personal data and processing delimit the application of the GDPR. Article 4 provides both definitions. Personal data and processing mean, respectively:

"any information relating to and identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly"; and

[29] Article 8(1) GDPR.
[30] Article 2(1) ibidem.

"any operation or set of operations which is performed on personal data, whether or not by automated means"[31]*;*

It is evident that the concept of persona data is broad, it includes subjective and objective information and the information related to a natural person "*by content, purpose or effect*"[32].

5.4.2.2 Actors and definitions under the GDPR

The relevant entities of the GDPR are data controllers, data processors and data subjects[33]. Succinctly, the data controller is the natural or legal person which – alone or jointly with others – determines the purpose and means of the processing of personal data. The data processor is the natural or legal person which processes personal data on behalf of the controller. Lastly, the data subject is a natural person who can be identified, directly or indirectly through the personal data.[34]

Another actor introduced by the GDPR is the Data Protection Officer (DPO). The DPO acts in independence inside an organization and refers directly to the board or management of that organisation. Under the GDPR, the role of the DPO is to oversee the application of data protection rules, procedures and policies. DPOs are also responsible for the effective enforcement of data subjects' rights[35].

5.4.2.3 Data protection principles under the GDPR

The GDPR provides a set of rights for the data subject. These concern e.g. transparency, information and access to personal data by the data subject, the right to rectification and the right to erasure.

When it comes to data protection principles, the GDPR expands international and primary sources that established the framework for the EU legislation on data protection. The vital principles worth mentioning are the following:

- Purpose limitation;
- Fairness, lawfulness and transparency;
- Data minimisation;
- Data accuracy;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

[31] Article 4(1)(2) GDPR.
[32] Article 29 Working Party, "Opinion 4/2007 on the concept of personal data", 20 June 2007, p. 10-11.
[33] Article 4(7)(8) GDPR.
[34] Article 4(1) GDPR.
[35] Article 39 ibidem.

The practical requirements of some of those principles were described in WP9 deliverables and will be further developed in D6.3 which deals with legal requirements for TRUSTS's platform development and later on also in deliverable D6.4, which will present the results of the mapping and analysis and provide recommendations at the end of the lifespan of the TRUSTS project. For now, a few general remarks are in order. The purpose limitation principles require that personal data can be collected for pre-determined and specific purposes, any processing outside of the original purpose is thus prohibited unless exceptions apply, such as e.g. Article 89 GDPR for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Fairness is hard to define and points to the ethical dimension of data protection (see above), whereas lawfulness requires that a lawful basis must exist for the processing of personal data. Lawful basis' for the processing of personal data are enumerated in Article 6 and are fulfilled when:

- The data subject consents to the processing for one or more specific purposes;
- The processing is necessary for the performance of the contract or in the pre-contractual phase (the data subject being one of the parties to the contract);
- The processing is necessary to comply with a legal obligation to which the controller is subject;
- The processing is necessary to protect the vital interest of the data subject or of someone else;
- The processing is justified for the public interest; or
- A legitimate interest pursued by the processor or a third party justifies the processing.

The principles governing the gathering and processing of personal data can be described jointly. Data minimisation requires that the personal data is processed (and acquired) to the extent that it is necessary for the purpose of the processing. Data accuracy requires that personal data contain correct information about the data subject and that must be kept up to date. Storage limitation is a corollary of the principle of purpose limitation to the extent that requires personal data to be kept in a form which allows identification for no longer than necessary. This criterion is evaluated on a case-by-case analysis based on the purpose of the processing. Lastly, integrity and confidentiality require appropriate technical and organisational measures to safeguard personal data from – amongst other things – unauthorised access, accidental loss, tampering, destruction or damage by implementing.

The principle of accountability, at last, requires the controller to demonstrate the compliance with the fundamental principles of data protection outlined above. Controllers are required to proactively demonstrate their compliance with the GDPR and this entails that the respect of the principles discussed above must be explicit in the data protection policy of the controller.

5.4.2.4 The principle of accountability and TRUSTS

Following the discussion in the paragraphs above, one aspect worth discussing already in this deliverable concerns the accountability measures introduced by the GDPR and how they relate to TRUSTS. Within the GDPR, accountability refers to the capacity of an organisation to demonstrate compliance, which entails that data controllers should adopt internal policies and documents aimed at ensuring compliance with the provisions that apply. Examples of the appropriate policies and documents include, but are not limited to, the following:

- Data protection policy;
- Privacy notice;
- Staff training policy;
- Information security policy;
- Data protection impact assessment procedure;
- Retention of records procedures;
- Procedures to comply with data subjects' rights;
- International data transfer procedure;
- Data portability procedures; and
- Complaints procedure.

The partners of TRUSTS have committed to apply the highest standards of data protection throughout the project, thus it is recommended that each partner assesses which policies are necessary to develop or update in their specific case in order to ensure compliance under the GDPR.

5.4.2.5 The rights of the data subject

The GDPR establishes several rights in favour of data subjects. Controllers have an obligation to facilitate the exercise of these rights and, under the transparency principle, communicate appropriately with the data subjects on matters related to such rights. More precisely, articles 12,13 and 14 describe the information to be provided by the controller to the data subjects which is aimed at ensuring that the data subjects can effectively exercise the rights granted under the GDPR[36]. Moreover, these dispositions aim at ensuring that the processing of personal data unfolds in a fair and transparent fashion.

The data subjects' rights are found in articles 15 to 22. They are:

- *Right of access;*
- *Right to rectification;*
- *Right to erasure;*
- *Right to restriction of processing;*
- *Right to data portability;*
- *Right to object*[37]*;*
- *Right not to be subject to a decision based solely on automated processing.*

[36] This is evident when considering article 13(2)(b) which states that the controller shall provide the data subject with information regarding "*the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability*".

[37] In situation related to the processing justified by public interest or the legitimate interest of the controller or a third party, this right includes the possibility to object to profiling in the aforementioned cases.

5.4.2.6 Security, integrity and managing data breaches

For the scope of this report, security measures introduced by the GDPR with regard to personal data are also worth mentioning. Article 5(f) reads:

"[personal data shall be] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"

Article 5(f) establishes the principles of integrity of confidentiality of personal data. On this basis, adherence to information security standards for the technical side of TRUSTS is desirable as it enhances the security of personal data. Article 32 goes into more details on the security of personal data, it includes both technical and organisational measures such as:

- Pseudonymization and encryption of personal data;
- Measures for the reliance of services and systems;
- Safeguards against cyber and physical incidents;
- Policies for the testing of such measures.

The principles of security and integrity follow a risk-based approach, for example that the appropriate implementation of the abovementioned mitigation strategies must take into consideration the costs, the state-of-the-art, the nature, and scope of data processing operations. The interplay of these factors in the context of TRUSTS will be thoroughly evaluated in T.8.5, more precisely it will form a central part of the data protection impact assessment of the pilots.

Another relevant aspect of the GDPR are the procedures for managing data breaches. The relevant dispositions are Articles 33 and 34 which deal with the duty of processors to inform the supervisory authority and data subjects respectively in case of data breaches. In the former case, data processors must notify the authority within 72 hours from the discovery of the data breach[38]; the content of this communication are the following:

- Nature of the breach, estimation of the data subjects and the number of personal data concerned;
- Contacts of the DPO;
- Likely consequences of the data breach;
- Measures adopted to recover from the data breach.

A notification of the data breach to data subjects is required if the data breach is likely to result in a high risk to the rights and freedoms of natural persons. This communication, which should occur in clear and plain language, is not required in three cases:

- Appropriate measures have been taken and the initial security has been restored;

[38] It is worth mentioning that the GDPR allocates to the controller the assessment of the gravity of the data breach, more precisely article 33(1) deems the notification necessary "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

- The high risk is no longer present;
- A disproportionate effort is required.

In the last case, controllers shall replace individual notifications with (effective) public communication.

5.4.2.7 International transfers of personal data

Furthermore, the GDPR describes the conditions for the legitimate international transfer of personal data[39]. As it has been described above, C108 and C108+ established the core principle of the necessity of adequate safeguards present in the jurisdiction where personal data are transferred. The GDPR goes into more details by specifying the conditions under which the transfer of personal data can occur to a third country or international organisation[40].

There are two cases in which the transfer of personal data is allowed. The first one is established by Article 45, rubricated "*transfers on the basis of an adequacy decision*". Under this provision, the transfer is allowed if the Commission has adopted an adequacy decision, confirming that the jurisdiction where the data are transferred ensures an adequate level of protection. The European Commission has already adopted the adequacy decision with Israel in 2011[41]. Therefore, the Adequacy decision is the relevant provision for TRUSTS.

Pursuant to Article 1 of the Adequacy decision, Israel is considered to provide an adequate level of protection for personal data transferred from the European Union. Pursuant to Article 3 of the Adequacy Decision with Israel, supervisory authorities in Member States may suspend data flows to a recipient in the State of Israel in order to protect individuals with regard to the processing of their personal data in the following cases:

a) where there is in breach of the applicable standards of protection;
b) where there is a substantial likelihood that the standards of protection are being infringed.

There are also a number of instruments that may provide appropriate safeguards. These are:

- A legally binding and enforceable instrument between public authorities or bodies;
- Binding corporate rules;
- Standard data protection clauses adopted by the Commission;
- Standard data protection clauses adopted by an authority and approved by the Commission;

[39] Please note that the notion of transfer is broad and it includes the access to personal data by an entity established outside the territorial scope of the GDPR.
[40] Under the GDPR third country means a country where the GDPR does not have direct application, in the case of TRUSTS, Israel is considered a third country.
[41] 2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332) OJ L 27, 1.2.2011, p. 39–42.

- An approved code of conduct; and
- An approved certification mechanism.

In these cases, the transfer can occur without previous authorization from the competent data protection authority. There are, however, two cases in which the cross-border transfer may occur subject to authorization from the competent supervisory authority. These cases regard contractual clauses between the controller and the processor and provisions to be inserted in administrative agreements between public bodies or authorities.

5.4.3 The ePrivacy Directive

The general obligations derived from the ePrivacy Directive apply to the processing of personal data with regards to the provision of publicly available electronic communications services in public communications networks in the EU.[42] It shall be also noticed that ePrivacy Directive' material scope of application is more extensive and goes beyond electronic communications service providers to include the cookie provision. However, it remains until now very unclear how to interpret this provision and especially how it relates to the GDPR.

An electronic communications service is defined as "*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.*"[43]

The data analytics tools as described in the TRUSTS use-cases do not fall within the scope of this definition, since they do not involve *"wholly or mainly in the conveyance of signals"*. The primary function of the TRUSTS data analytics tools is to perform analytics on data and data service, rather than the conveyance of signals. Consequently, most obligations that apply to providers of electronic communications services will not be applicable to the use-cases of the TRUSTS project.

At the same time, the concept of consent under the ePrivacy Directive is the same as under the GDPR, meaning that consent must be freely given, specific, informed, and unambiguous.[44] The user must also

[42] ePrivacy Directive, Art. 3.
[43] ePrivacy Directive, Art. 2.
[44] ePrivacy Directive, recital 17; GDPR, Art. 94; GDPR, Rec. 32.

receive clear and comprehensive information in accordance with the GDPR, including about the purposes of processing. For more in-depth analysis of the ePrivacy Directive and its intersection with the GDPR we refer to our Deliverable D6.2.

5.4.4 The ePrivacy Regulation

It is worth mentioning that on the 10th of January 2017, the European Commission released its proposal for a new ePrivacy Regulation[45] replacing the 2002 ePrivacy Directive in the electronic communication sector.

On 10 February 2021, member states agreed on a negotiating mandate for revised rules on the protection of privacy and confidentiality in the use of electronic communications services.[46] These updated 'ePrivacy' rules will define cases in which service providers are allowed to process electronic communications data or have access to data stored on end-users' devices. The upcoming legislative process will involve negotiations with the European Parliament on the final text.

The draft ePrivacy regulation, if adopted, will repeal the existing ePrivacy directive. As *lex specialis* to the general data protection regulation (GDPR), it will particularise and complement the GDPR. For example, in contrast to the GDPR, many ePrivacy provisions will apply to both natural and legal persons. In its current shape, the Regulation covers electronic communications content transmitted using publicly available services and networks, and metadata[47] related to communication. The processing of metadata without consent is only allowed in certain cases related to information security, fraud prevention, service provision (for example, billing and managing abuse of the service) or for the protection of "vital interests" which follows the same concept used in the GDPR. In line with the purpose limitation principle set out in the GDPR, the Council's draft provides that pseudonymised metadata can be processed for purposes other than those for which it was collected, provided such processes are "compatible" with the original purpose.

The proposal also includes rules on Internet of Things to cover machine-to-machine data transmitted via a public network. The Regulation also contains rules on cookies. As a general rule, the end-user should have a genuine choice on whether to accept cookies or similar identifiers. The so-called "cookie consent fatigue" has also been addressed, giving an end-user a choice to consent to the use of certain types of

[45] See, for the original text proposed by the European Commission: Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC ('ePrivacy Regulation') (2017) 2017/0003(COD) <http://data.consilium.europa.eu/doc/document/ST-5358-2017-INIT/en/pdf> accessed 3 April 2018.

[46] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP; available at: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf.

[47] Metadata includes, for example, information on location and the time and recipient of communication.

cookies by whitelisting one or several providers in their browser settings. The text also includes rules on line identification, public directories, and unsolicited and direct marketing.

At this stage it is rather unclear how the final draft of the Regulation will look like. The trialogue process still has to start. It will have to be further analysed what are the practical implications of the upcoming Regulation on TRUSTS project.

6 Research ethics as applied in TRUSTS: step-by-step explanation

In order to ensure compliance of TRUSTS project with "ethics requirements" described in the Grant Agreement, the following process has been set up:

- A questionnaire (Annex I) was drawn and circulated amongst all TRUSTS partners (27th March 2020). It was accompanied by a Background Note providing further explanation on applicable data protection legal provisions in order to ease the filling of the questionnaire. The filling of the questionnaire was use case-specific.
- 3 questionnaires were drawn, namely one questionnaire for every use case as coordinated by respective use case leaders.
- A virtual meeting was convened (15th April 2020) to have a general discussion between partners on the ethics requirements and on how to comply with them.
- A virtual meeting was convened for every use case (21st April and 24th April 2020) in order to tailor the ethics deliverables.
- Based on the information gathered through the questionnaires and the virtual meetings, a first version of the ethics deliverables was drawn and circulated amongst the partners (18th May 2020).
- After internal review amongst TRUSTS partners, the ethics deliverables were submitted to the European Commission at the end of June.

Ethics deliverables shall be considered as a consistent set of measures aimed at ensuring compliance with ethics requirements within the TRUSTS project. Finally, compliance with ethics and legal requirements is considered as continued effort by the partners to be maintained throughout the project. In this section, KUL will remind the TRUSTS partners of the main data protection and ethics related concepts from the Background note relevant for the project lifecycle.

6.1 Background note

What is 'personal data' within the meaning of data protection law?

Article 4(1) GDPR defines 'personal data' as '*any information relating to an identified or identifiable natural person ('data subject')*'. The notion of 'identifiable natural person' is clarified as meaning a

natural person '*who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*'. In order to contribute to a uniform interpretation of the notion of "personal data", the Article 29 Working Party[48] adopted an opinion clarifying the elements of this concept.[49] The opinion adheres to the broad notion of 'personal data' adopted by the Council of Europe's Convention 108[50] which allows room for a flexible and future-proof reading of that notion. The document highlights that the scope of data protection rules should not be overstretched at the risk of ending up applying data protection rules to situations which were not intended to be covered by those rules and for which they were not designed by the legislator. The opinion identifies four main components of the definition.[51]

a) First, the notion of personal data includes 'any information'

While the Working Party does not provide a definition of 'information', it focuses on the types of information that would fall within the ambit of personal data.[52] The opinion clarifies that **the *nature* of a piece of information is irrelevant** to the assessment of whether it refers to personal data or not. This means that any kind of statement about a person, **whether objective** (*e.g.,* the presence of a certain substance in one's blood) **or subjective** (e.g., behavior of a customer when dealing with a call center), **true or not proven**, may be considered as personal data. Equally **irrelevant is the *content* of the information,** i.e. the concept is not limited to information that refers to an individual's private and family life but also includes information on whatever types of activity is undertaken by her (e.g*.,* information concerning a person's working relations or his/her economic and social behavior).[53] Finally, t**he medium or format in which the information is contained are also irrelevant** (e.g*.,* data kept on paper or stored in a computer memory or on a tape).[54] This very broad approach to information brings virtually unlimited number of categories of data within the ambit of personal data,[55] an understanding also reflected in the ruling in the *Nowak* case.[56]

[48] Now the European Data Protection Board.
[49] Article 29 Working Party, 'Opinion 4/2007 on the concept of personal data' (WP136).
[50] Recently updated by the Council of Europe. See more at: https://www.coe.int/en/web/portal/-/enhancing-data-protection-globally-council-of-europe-updates-its-landmark-convention.
[51] For streamlined information on the notion of personal data under the GPDR, see *a.o.*: (Ustaran 2018, 60–64).
[52] For an in-depth analysis of the notion of 'information', see: (Purtova 2017, 8–12).
[53] Private and family life, home and communications/correspondence is rather the scope of application of the fundamental right to privacy as stated in Article 8 ECHR and Article 7 CFREU. This notion has also been interpreted very widely. See: ECtHR, *Amann v. Switzerland*, n. 27798/95, ECHR 2000-II, para. 65. In that sense, personal data might also fall under the scope of the right to privacy. It is, however, not necessarily the case.
[54] On technological neutrality, see recital 15 GDPR: '*the protection of natural persons should be technologically neutral and should not depend on the techniques used*'.
[55] Purtova (n 49) 10. Also see references 59 and 60 therein.
[56] CJEU, *Peter Nowak v. Data Protection Commissioner*, case C-434/16, para. 46.

b) Second, the information must 'relate to' an individual

The Article 29 Working Party interprets this notion as meaning that the information at stake is *about* that individual. In other words, **an assessment must be made of the relationship between a specific piece of information and a person**. Often, this link appears self-evident (e.g., employe's personal file kept by the human resources department). In others, whenever the information relates to objects, processes or events, this may not be so obvious (e.g., the value of a house which, while being about a material object rather than a person, still conveys meaningful information about its owner's wealth).[57] The Article 29 Working Party sets out three alternative criteria for a certain piece of information to 'relate' to a person: (1) *content* (i.e., when the data are about a person), (2) *purpose* (i.e., when the data are used or are likely to be used with the purpose to evaluate, treat in a certain way or influence the status or behavior of that person)[58] or (3) *result* (i.e., when the data used are likely to have an impact on that person's rights and interests). It follows that one and the same piece of information may relate to different individuals at the same time, depending on which element can be identified in regard to which person.

c) Third, the information must relate to an 'identified or identifiable' person.

The Article 29 Working Party interprets this as meaning that an individual is *identified* when, within a group of persons, she is **distinguished from all other members of the group**. On the other hand, *identifiable* means that, although the person has not been identified yet, it is still possible to do so. The Article 29 Working Party also distinguishes between *directly* and *indirectly* identified or identifiable. While in the former case reference is made to a name (in combination with additional information if the name is not unique), the latter refers to the so-called 'unique combination' phenomenon that allows the singling out of the person on the basis of multiple pieces of information, whether retained by the controller or not. To ascertain whether an individual is identifiable, recital 26 GDPR specifies that '*account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly*'. The means reasonably likely to be used must be assessed in light of '*objective factors, such as the costs of and the*

[57] In that specific context, the Article 29 Working Party specifies that data protection rules wouldn't apply to such information when it is used solely to illustrate the level of real estate prices in a certain area.

[58] Strangely the CJEU, in its *YS and Others v. Minister voor Immigratie* case law, denied the qualification of personal data for the legal analysis within the minutes of immigration files. Despite such a reasoning being used '*with the purpose to evaluate, treat in a certain way or influence the status or behaviour of that person*', judges still concluded that it does not itself constitute personal data. See CJEU, *YS and Others v. Minister voor Immigratie*, case C-141/12, para 39. This interpretation goes against the approach suggested by the Working Party. On the contrary – and in accordance with the Working Party –, the CJEU ruled that the exam script containing a candidate's answers must be considered as personal data, as '*the aim of the examination is to identify and record the performance of a particular individual*'. See CJEU, *Peter Nowak v. data Protection Commissioner*, case C-434/16, para. 24. As such, it used '*with the purpose to evaluate, treat in a certain way or influence the status or behaviour of that person*'.

amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments'. This has led to the CJEU's ruling that dynamic IP addresses could also constitute personal data since they can potentially be combined with data held by internet service providers to allow identification of the user.[59] This means that establishing the identifiability of the person, and consequently the applicability of the GDPR, requires a dynamic, context-sensitive analysis of the factual situation.[60] Thus, **the exact same dataset might be considered as not personal at the start of the processing and, later on, fall under the definition of 'personal data' given the tools and data available to the controller.[61] The same might happen depending on who is actually processing the datasets**.

This building block is of utmost importance in the context of analytics tools and methods which allow for combinations of data originating from various sources. While the identifiability of an individual might previously have appeared as limiting the applicability of data protection rules, this is likely to change given the growing data availability and the evolution of analytic technologies.[62] Both of these factors

[59] Here the fact that it was legally possible for the website to request access to the corresponding identifier within the internet service provider's database was enough to qualify the dynamic IP address as relating to an 'identifiable' person'. The Court, however, somehow rejected – although not in clear terms – the 'objective/absolute' approach according to which data is already considered to be 'personal' if any third party worldwide is able to determine the identity of the individual. See: CJEU, *Patrick Breyer v. Bundesrepublik Deutschland*, case C-582/14, para. 31-49. See also, on static IP addresses: CJEU, *Scarlet Extended SA v. SABAM*, case C-70/10, para. 29-54. On that point, see: (Nemiann and Schüßler n.d.)

[60] *Dynamic* because the objective factors mentioned, as well as the likelihood of the means to be used by the controller, may vary over time (*e.g.* growing evolution of BDA tools and methodologies allowing for easier, quicker identification of individuals on the basis of a combination of various information, deletion of the additional information precluding any risk of identification, etc.) and *context-sensitive* because the identifiability of the individual must be assessed in light of the purpose pursued by the controller in the data processing; if it implies the identification of the individuals, the Working Party notes, '*it can be assumed that the controller or any other person involved have or will have the means "likely reasonably to be used" to identify the data subject*'.

[61] Purtova 2017, 7; Koops 2014, 4.

[62] In practice, it has already been demonstrated that very basic, or at least partially 'anonymised' data, may be linked to a person without much effort . In that sense, see *a.o.*: Larry Hardesty, 'It's Surprisingly Easy to Identify Individuals from Credit-Card Metadata' (*MIT News*, 29 January 2015) <https://news.mit.edu/2015/identify-from-credit-card-metadata-0129> accessed 8 February 2018; Latanya Sweeney, 'Simple Demographics Often Identify People Uniquely' Carnegie Mellon University, Data Privacy Working Paper <https://dataprivacylab.org/projects/identifiability/ paper1.pdf> accessed 19 March 2018; Arvind Narayanan and Vitaly Shmatikov, 'Robust De-Anonymization of Large Sparse Datasets' (IEEE 2008) <http://ieeexplore.ieee.org/document/4531148/> accessed 19 March 2018; John Bohannon, 'Credit Card Study Blows Holes in Anonymity' (2015) 347 Science 468; JK Trotter, 'Public NYC Taxicab Database Lets You See How Celebrities Tip' (*Gawker*) <http://gawker.com/the-public-nyc-taxicab-database-that-accidentally-track-1646724546> accessed 19 March 2018.

increase the likelihood of someone being able to link a specific information to a person, triggering the applicability of the GDPR.[63]

6.2 Pseudonymisation and anonymisation within the meaning of the GDPR.

GDPR applies to pseudonymized data defined by Article 4(5) GDPR as '*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*'. The Article 29 Working Party points out that **pseudonymization is about disguising the identity of data subjects so that information can be collected without having to know their name, which proves particularly relevant in the context of research and statistics**. This can be done in:

- a retraceable way, e.g., using correspondence lists or two-way cryptography algorithms, or
- in a non-retraceable way, e.g., using one-way cryptography algorithms.

In the first case, individuals are still indirectly identifiable since it is possible to backtrack their identity using additional information, so such data will still be considered personal within the GDPR's scope of application.[64] **In the second case, individuals are no longer identifiable** since the link between their pseudonym and identity is either inexistent or has been permanently deleted. Such non-retraceable pseudonymization techniques generally create **anonymized data** that are not subject to data protection rules.

The key criterion in distinguishing pseudonymized data from anonymized data is whether individuals are identifiable. In turn, this hints at the need to assess the '**means reasonably likely to be used by the controller or another person**'. Depending on the context of the processing, the technology used to separate identifiers from raw datasets and the undertaking which is actually processing the data, the outcome of such an assessment may vary. This calls for a case-by-case analysis of the factual circumstances surrounding the processing operations.

Another important distinction concerns the anonymization of personal data. Recital 26 GDPR states that '*the principles of data protection **should not apply** to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous **in such a manner that the data subject is not or no longer identifiable***'. This reflects the case-by-case

[63] Recital 14 GDPR.

[64] This is confirmed by Recital 26 GDPR which states that 'personal data which have undergone pseudonymisation, which could be *attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person*'.

assessment that must be carried out to ascertain whether or not individuals remain identifiable given the 'means reasonably likely to be used' to do so. If identification is no longer possible, data will be considered as anonymized and as such will fall outside the GDPR's scope of application. However, if it is still possible to identify the natural person to whom the data relate, the data(sets) at stake will still be considered as personal data.

The Article 29 Working Party acknowledges in another opinion that the creation of a truly anonymized dataset from a rich assortment of personal data whilst not depriving the information it carries from its added value is not a trivial task.[65] It highlights that in determining whether or not the data are still identifiable, **focus should be placed on the concrete means that would be necessary to reverse the anonymization technique**, particularly the knowledge how to implement those means and the assessment of their likelihood and severity. Additionally, one must bear in mind that **the means to be assessed are not only those of the controller, but also the ones that may be used by any other person**.[66] True anonymization is consequently a very onerous standard, and the notion calls for vigilance when used.

6.3 What is 'sensitive data' within the meaning of the GDPR and why does it matter?

The GDPR lays down specific – stricter - provisions for the protection of the so-called "sensitive data", namely (1) **"special categories of personal data"** within the meaning of Art. 9 GDPR and (2) "**personal data relating to criminal convictions and offences**" within the meaning of Art. 10 GDPR.

a) Special categories of personal data

Special categories of personal data include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data

[65] Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (WP 216).

[66] The Working Party underlines that, '*when a data controller does not delete the original (identifiable) data at event-level, and the data controller hands over part of this dataset (for example after removal or masking of identifiable data), the resulting dataset is still personal data*'. It adds that '*only if the data controller would aggregate the data to a level where the individual events are no longer identifiable, the resulting dataset can be qualified as anonymous*'. It adds: '*if an organisation collects data on individual travel movements, the individual travel patterns at event level would still qualify as personal data for any party, as long as the data controller (or any other party) still has access to the original raw data, even if direct identifiers have been removed from the set provided to third parties. But if the data controller would delete the raw data, and only provide aggregate statistics to third parties on a high level, such as 'on Mondays on trajectory X there are 160% more passengers than on Tuesdays', that would qualify as anonymous data*'.

concerning a natural person's sex life or sexual orientation".[67] The processing of such data is in principle prohibited. It can however be expected to this principle, pursuant to the conditions laid down in Article 9 (2) GDPR, such as in case the data subject has given explicit consent, except where EU or national law provides otherwise,[68] or in cases where the processing relates to personal data which are "manifestly made public by the data subject".[69] The prohibition of such sensitive data processing may also be overridden in cases where necessary for, notably, **scientific research purposes**, where based on EU or national law and subject to specific legal safeguards.[70]

Amongst these special categories of personal data, genetic data, biometric data and data concerning health are singled out, as **Member States can further regulate the processing**.[71]

b) Personal data relating to criminal convictions and offences

According to Article 10 GDPR, the processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorized by EU or national law. Such legal framework shall provide for appropriate safeguards for the rights and freedoms of data subjects. Additionally, any comprehensive register of criminal convictions shall be kept only under the control of official authority.

Furthermore, as clarified by the CJEU in the *GC and Others v CNIL* case, information (ie newspaper articles) on judicial investigations, trials and ensuing convictions shall be considered as data relating to offences and criminal convictions within the meaning of Article 10 of the GDPR.[72]

6.4 What is lawfulness and lawful basis within the meaning of the GDPR?

Art. 5 (1) (a) states as one of the core principles of personal data processing, that it should be "lawful". Art. 6 ("lawfulness of processing") further clarifies that 'lawfulness' refers to the obligation to have a legitimate basis to conduct the data processing, amongst those listed in the GDPR. In other words, processing personal data is lawful only provided it is based on a legitimate ground.

(a) "Consent"

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*" (Art. 4 (11)). These high standards principles are

[67] GDPR, Art. 9 (1).
[68] GDPR, Art. 9 (2) (a).
[69] GDPR, Art. 9 (2) (e).
[70] GDPR, Art. 9 (2) (j).
[71] GDPR, Art. 9 (4).
[72] C-136/17 GC and Others v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:773, para 72.

complemented with more specific clarifications. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (Art. 7 (2)). In the case of sensitive data, consent must even be **explicit** (Art. 9(2)(a)). If the data subject's consent is requested by electronic means, this request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided (Rec. 32).

The CJEU clarified that pre-ticked boxes fail to qualify as valid consent within the meaning of the GDPR, which requires 'an active behaviour with a clear intention on the part of the data subject to consent to the data processing.[73]

The notion "freely given" implies genuine choice and control for data subjects.[74] The use of enticements, inducements or rewards to elicit consent may call into question the extent to which such consent is 'freely-given'.[75] The requirement that consent is "freely given" also implies that consent can be **freely withdrawn by the data subject, at any time** (Art. 7 (3)). Furthermore, the consent is not deemed as "freely given" when bundled to contracts or the provision of a service as described in Article 7(4). This legal requirement also implies that "utmost account' shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the personal data processing that is **not necessary** for the performance of the contract (Art. 7 (4)). In order to assess whether such bundling or tying occurs, it is important to determine the scope of the contract and what data would be necessary for its performance.[76] The notion "necessary for the performance of a contract" needs to be interpreted strictly.[77] For instance, the data may be necessary to fulfil the contract for example, processing the address of the data subject so that goods purchased online can be delivered, or processing credit card details in order to facilitate payment.

Recital 43 clarifies that there is **a presumption of consent not being freely given** if "it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service is dependent on the consent **despite such consent not being necessary for such performance**". Consent and purpose are intrinsically related. Transparent and **simple explanation of the purpose(s)** of the processing of personal data allows a data subject to make an informed decision. Consent should "cover all processing activities carried out **for the same purpose or purposes**". This also means that "when the processing has multiple purposes, consent should be given **for all of them**" (Rec. 32).

[73] CJEU, C-673/17, *Planet49*, judgment of 1 October 2019, para 52 and 54.
[74] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, pp. 5-7.
[75] EDPS, 'A Preliminary Opinion on data protection and scientific research', 6 January 2020, p. 18.
[76] Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (WP259), 8.
[77] Ibid.

(b) "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract"

Processing based on this legal basis must be necessary for the performance of the contract or for addressing the pre-contractual request to be able to process the personal data on the 'contract' legal basis. This necessity limits the amount of personal data that can be lawfully processed under the 'contract' legal basis. Which personal data are necessary shall be determined on a case-by-case basis. Personal data that is not strictly necessary for these purposes, shall only be processed if another legal basis for such processing is available.

(c) "Processing is necessary for compliance with a legal obligation to which the controller is subject"

The legal obligation can be laid down either in EU or in national law, to which the controller is subject. While the GDPR does not require a specific law for each individual processing, **the law should determine the purpose of processing**, in order to qualify as lawful ground (Art. 6 (3)). The law may also further specify the general conditions of the processing, such as the entities to which the personal data may be disclosed, the purpose limitations, the storage period, types of data processed etc. (Rec. 45).

(d) "Processing is necessary in order to protect the vital interests of the data subject or of another natural person"

The 'vital interests' lawful basis is to be used exceptionally, in actual situations of emergency, for example if someone is in danger. Thus, it shall not justify regular processing activities.

(e) "Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

In such a case, there should be a basis in either EU or Member State law (Art. 6 (3)) whether the controller performing such a task in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so by private law. Just like for personal data processing activities based on a legal obligation, the GDPR does not require a specific law for each individual processing, but the law should **determine the purpose of processing** (Rec. 45).

(f) "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data […]"

It should be observed at the outset that such a legal ground cannot be invoked by public authorities for processing carried out in the performance of their tasks.

While the GDPR does not provide an exhaustive list of what could constitute a "legitimate interest" – or in other words which (commercial) interest could qualify as legitimate – Rec. 47 clarifies that there could for example be a legitimate interest "where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller".

The "legitimate interest ground" implies a balancing exercise between the legitimate interest of the controller (or third party) and the rights and freedoms of data subjects. In doing the balancing exercise, consideration shall be taken to the "reasonable expectations of data subjects based on their relationship with the controller". The GDPR does also not provide much further clarification of the circumstances in which the rights and freedoms of individuals would override the legitimate interest of the controller (or third party). Such balancing exercise remains therefore much context-specific.

The lawfulness legal requirement can be summarised by the following figure:

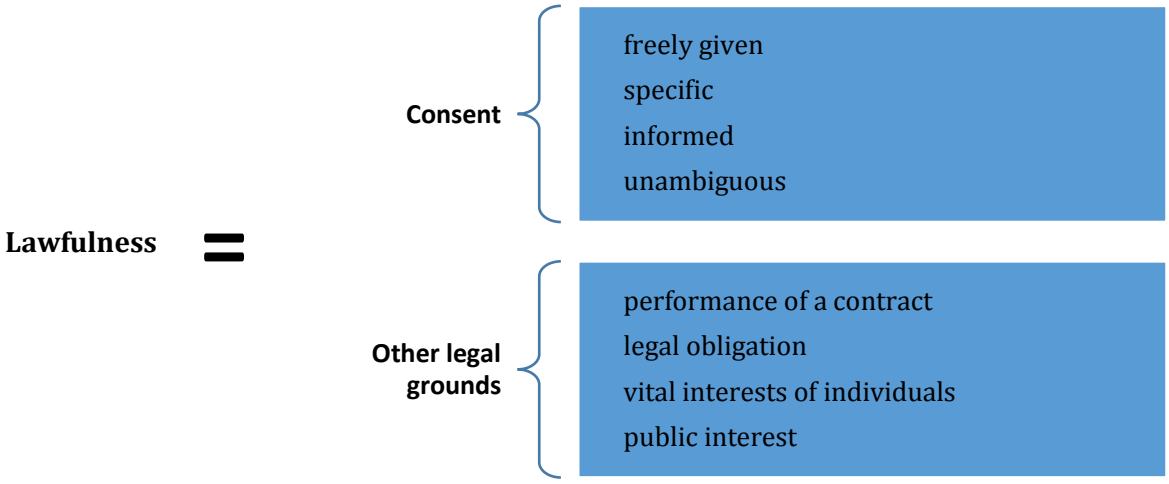


Figure 1: The lawfulness legal requirement

6.5 The purpose limitation principle

Article 5(1)b GDPR stipulates that personal data shall be '*collected for* ***specified, explicit and legitimate purposes*** *and* ***not further processed in a manner that is incompatible with those purposes****; further*

processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'.

The Article 29 Working Party has identified two main components of this principle, which have a role to play at different moments of the processing of personal data:

a) Personal data may be collected only for specified, explicit and legitimate purposes.

This means that the data should correspond to the aims justifying their **collection** (e.g., collection of a postal address in order to proceed with a delivery). It can be inferred that the purposes must be specified, i.e. sufficiently defined, prior to, and in any event, not later than, the time when the collection of personal data occurs.[78] The purposes must also be explicit, that is to say, sufficiently unambiguous and clearly expressed. Finally, they must be legitimate in the sense that they must match the legal expectations of data subjects (not to be confused with lawfulness).

b) Personal data collected for these purposes should not be 'further processed' in a manner which is incompatible with them.

In principle, further processing, namely processing the data for another purpose than the purpose for which they were initially collected – should however be allowed **where compatible with the initial purpose(s)** (Recital 50 GDPR), as illustrated by the following figure. Therefore, when personal data are further used for compatible purposes, 'no legal basis separate from that which allows the collection of the personal data is required'.[79] This is based on 'the reasonable expectations of data subjects based on their relationship with the controller as to the data's further use' (Recital 50 GDPR).

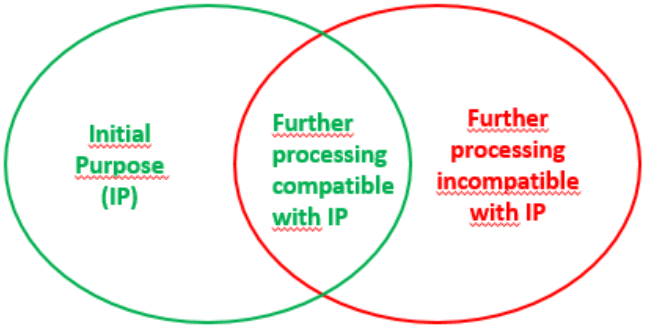


Figure 2: Further processing

This requires an assessment of compatibility based on several criteria laid down in Recital 50 GDPR, namely: (1) the **link between the purposes** for which the data have been collected and the purposes of

[78] Article 29 Working Party, 'Opinion 03/2013 on purpose limitation', p.15.
[79] EDPS, 'A Preliminary Opinion on data protection and scientific research', 6 January 2020, p. 22.

further processing, (2) the **context** in which the data have been collected and the reasonable expectations of the data subjects as to their further use, (3) the **nature** of the personal data and the impact of the further processing on data subjects and (4) the **safeguards** applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.[80] In such a case and in line with the principle of accountability, **it is for the controller to demonstrate that the further processing is indeed compatible with the initial one, on a case by case basis**.

The **further processing is however considered by default compatible** with the initial purpose in three different types of situations:

i. The further processing is **based on data subject's consent** (within the meaning described above) (Art. 6 (4));

   The further processing is **based on EU / national law** which constitutes a **necessary and proportionate measure in a democratic society** to safeguard one of the following objectives: national security; defense; public security; the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest of the EU or of a Member State, in particular an important economic or financial interest of the EU or of a Member State, including monetary, budgetary and taxation matters, public health and social security; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to above; the protection of the data subject or the rights and freedoms of others; the enforcement of civil law claims (Art. 6 (4) and 23 (1)).

Further processing is **deemed compatible**[81] with initial purpose when undertaken for archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes, provided subject to appropriate safeguards for the rights and freedoms of the data subject(s), i.a. to ensure that technical and organisational measures are in place in particular to ensure respect to the principle of data minimization (e.g. pseudonymisation) (Art. 5 (1) (b) and 89 (1)).The further processing of personal data for scientific purposes is further discussed in the "scientific research purpose" section.

[80] As also follows from Article 6(4) GDPR.

[81] EDPS recently argued that, in order to ensure respect for the rights of the data subject, the compatibility test should still be considered for the purposes of scientific research, especially where the data was originally collected for very different purposes or outside the area of scientific research ('A Preliminary Opinion on data protection and scientific research', 6 January 2020, p. 23).

6.6 Legal regime for processing personal data for research purposes

Where it involves the processing of data concerning people in the EU, scientific research is subject to the applicable rules including the GDPR. The rules contain a special regime affording a degree of flexibility for genuine research projects that operate within an ethical framework.

There is no universally agreed definition of research or scientific research.[82] Not only academic researchers but also not-for-profit organizations, governmental institutions or profit-seeking commercial companies can carry out scientific research.[83] The GDPR introduced a **special regime for scientific research** which is composed of specific derogations from certain controller obligations plus a specific provision (Article 89) requiring appropriate safeguards.[84]

The GDPR distinguishes the two following situations with respect to personal data processed for scientific research purposes: (1) Data are initially obtained from the data subject(s) for scientific research purposes; (2) Data were initially collected for another purpose, and then further processed for scientific research purposes. This section brings little additional information to the other (preceding) sections, but aims to summarize on which lawful ground data processing can be conducted for scientific research purposes for the sake of clarity.

a) Data initially obtained from the data subject(s) for scientific research purposes

The GDPR **does not lay down a specific, separate lawful ground for data processing activities initially undertaken for scientific research purposes**. This means that, depending on the specific context of the data processing activities, one of the lawful grounds shall be identified, as provided for in:

- Art. 6;

On that aspect, please refer to the "lawfulness" section. In particular, the legitimate interest of the controller(s) or of a third party, could constitute a lawful ground (Article 6 (1) (f) where the data processing is necessary for such purpose. In that case, a balance should be made between the said legitimate interest(s) and the interests or fundamental rights and freedoms of the data subject(s).

The processing of personal data may also be considered 'necessary for the performance of a task carried out in the public interest' (Article 6(1)(e) GDPR) laid down by EU or Member State law. According to European case law, necessity and the public interest imply a 'pressing social need', as opposed to largely private or commercial advantages. Recently there have been calls for regulated access across the EU to personal data for research purposes that serve a public interest, noting the uncertainty around what counts as 'scientific research'. However, at this stage it is not clear how to interpret the 'public interest' in the context of scientific research.[85] It is important to mention that Member State and/ or Union law is needed in order to stipulate a legal obligation and/or a task carried out in the public interest under

[82] Rec. 157 and 159 GDPR. The role of research is understood to provide knowledge that can in turn improve the quality of life for a number of people and improve the efficiency of social services.
[83] EDPS, A Preliminary Opinion on data protection and scientific research p.11.
[84] Ibid.
[85] EDPS, 'A Preliminary Opinion on data protection and scientific research', 6 January 2020.

Article 6 GDPR. This implies that choices made in national laws can have a considerable impact on the legal basis (Article 6) that must be relied on when processing personal data, including for scientific research purposes. Therefore, Member States' law can have a serious impact on the extent to which personal data can be used for scientific research purposes.

- Art. 9, when dealing with sensitive data ("special categories of data").

The special regime applicable to sensitive personal data is as follows: in principle, their processing is **prohibited** under Article 9(1); this general prohibition is lifted only if one of the justifications enumerated in the Article 9(2) applies. Lawful processing of sensitive personal data must have a lawful basis (article 6 GDRP) for processing **and** one of the justifications of article 9(2) GDPR.

The list of justifications is exhaustive, meaning that if an entity processes a special category of personal data in any other situation not covered by Article 9(2), the processing is unlawful. The processing of other types of sensitive personal data, such as data related to prior criminal convictions, or location data, is often limited or even prohibited by other national or international rules.

Article 9(2)(a) permits to process special category if: "*the data subject has given explicit consent to the processing of those personal data for one or more specified purposes*". In particular, it must be freely given, specific, affirmative (opt-in) and unambiguous, and able to be withdrawn at any time.

The processing of "special categories of data" ('sensitive data'), when necessary for scientific research purposes, can be allowed based on EU or Member State law (Art. 9 (2) (j)) where subject to appropriate safeguards. However, such laws have yet to come into being.[86] Article 9(2)(e) permits to process special category data if: "processing relates to personal data which are manifestly made public by the data subject". Special categories of data may be processed if the data subject has **manifestly** made them public. "Manifestly" means that there must be clear evidence of a deliberate, affirmative act by the data subject themselves to make their data available.

Article 9(2)(j) permits to process special category data if the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The GDPR reckons that it may not be possible to "fully identify the purpose of personal data processing for scientific research purposes at the time of data collection".[87] This could constitute a severe obstacle to obtain consent within the meaning of the GDPR, which requires the consent to be given for "one or more *specific* purposes" (emphasis added).[88] For this reason, the GDPR provides for a possibility of a

[86] Recently there have been calls for regulated access across the EU to personal data for research purposes that serve a public interest, noting the uncertainty around what counts as 'scientific research'. (EDPS, 'A Preliminary Opinion on data protection and scientific research', 6 January 2020, p. 19).
[87] GDPR, Rec. 33.
[88] GDPR, Art. 6 (1) (a).

'**broad consent'**, which may be given by data subject(s) to "**certain areas of scientific research**" or "parts of research projects" while research should be conducted "with recognized ethical standards for scientific research".[89] When research purposes cannot be fully specified, the essence of the data subject rights to valid consent can be ensured through as much transparency as possible and other safeguards.[90] Although there might be overlaps between informed consent of human participants in research projects involving humans and consent under data protection law, they should not be viewed as a single and indivisible requirement. It would be simplistic and misleading as stated by the EDPS,[91] and might even constitute a form of bundled – or tied- consent.

b) Data were initially collected for another purposes, and then further processed for scientific research purposes

On that aspect, please refer to the "purpose limitation principle" section.

Any re-use of data for scientific research purposes, even if deemed to be compatible, would anyway require that the data were **initially** processed based **on a lawful ground**.

c) Safeguards under Article 89 GDPR

As mentioned above, further processing of personal data initially collected for another purpose is compliance with safeguards referred to in Art. 89 GDPR. Art. 89 (1) GDPR provides for the obligation to set up appropriate safeguards for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organizational measures are in place in particular in order to ensure respect for the principle of data minimization. Those measures may include pseudonymization provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. On anonymization and pseudonymization see section 6.2 above.

d) A note of caution

While the GDPR aims to harmonize the legal protection of personal data processing (as compared to the previous Data Protection Directive), **Member States may provide for derogations from some data subjects' rights**, namely the right of access (Art. 15), the right to rectification (Art. 16), the right to restriction of processing (Art. 18) and the right to object (Art. 21), subject to conditions and safeguards laid down in Article 89 (1) of the GDPR, and particularly technical and organizational measures to ensure data minimization. EU law could also, where appropriate, lay down specific regulation for scientific research.

[89] GDPR, Rec. 33.
[90] EDPS, 'A Preliminary Opinion on data protection and scientific research', 6 January 2020, p. 19.
[91] Ibid.

6.7 Data minimisation

Data minimisation is about asking whether the same purpose can be achieved with a narrower collection of data. Article 5(1)c GDPR therein requires to ensure that personal data are '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*'.

This essentially calls for a **necessity** and a **proportionality** test, against the purpose of data processing.[92] When it comes to necessity, controllers should make sure that they only process personal data that are suitable and reasonable to accomplish the purposes specified according to the purpose limitation principle (see *supra*). In other words, controllers should assess whether these purposes could be achieved with either less data or with properly anonymised datasets. As to the latter, it requires controllers to tailor the amount of data collected, as well as their retention period, to the identified purposes.[93] This also implies a need for putting in place adequate technical and organisational measures, for instance pseudonymisation.

In reality, it can be more complicated to perform the minimisation assessment **in the context of research activities**, since minimisation is **linked to the purposes** of the processing and **cannot be evaluated in the abstract**. Yet, it is often not possible to fully identify the purpose of personal data processing for scientific research activities at the time of data collection, as reckoned in the GDPR (Rec. 33, see also "scientific research" section).

For instance, collecting data other than payment details and postal addresses in the context of an online delivery would probably be seen as excessive with regard to the purpose of the product delivery.

6.8 What is a Data Protection Impact Assessment and when is it required?

While the Directive 95/46/EC (the Data Protection Directive, in force before the GDPR entered into force) provided for a general obligation to notify the processing of personal data to the supervisory authority(ies), the GDPR abolished such notification requirements with a view to tailoring data protection obligations depending on the severity of the risks to the rights and freedoms of individuals. (Recital 89 GDPR). Against this backdrop, where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a data protection impact assessment ('DPIA') within the meaning of Art. 35 GDPR.

a) In which cases are DPIA required?

[92] See Article 29 Working Party, 'Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector' (WP211).
[93] See Recital 39 GDPR: data minimisation '*requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum*'.

Carrying out a DPIA is required in three categories of situations:

(1) **The controller is explicitly required to do so by the GDPR, when he/she envisages:**

i. A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

ii. The processing on a large scale of "special categories of data" or of personal data relating to criminal convictions and offences ('sensitive data'); or

iii. A systematic monitoring of a publicly accessible area on a large scale.[94]

(2) The controller envisages data processing activities **identified on the list published by the national supervisory authority.**[95] Supervisory authorities may also issue a list of processing activities which do not require a DPIA (Art. 35 (5) GDPR).[96]

(3) The controller otherwise envisages processing of personal data, which **is likely to result in a high risk to the rights and freedoms of natural persons**, taking into account the nature, scope, context and purposes of the processing. This is especially so if "new technologies" are used,[97] but the **GDPR does not provide an exhaustive list of cases in which a DPIA is required, precisely in order to be future-proof**.

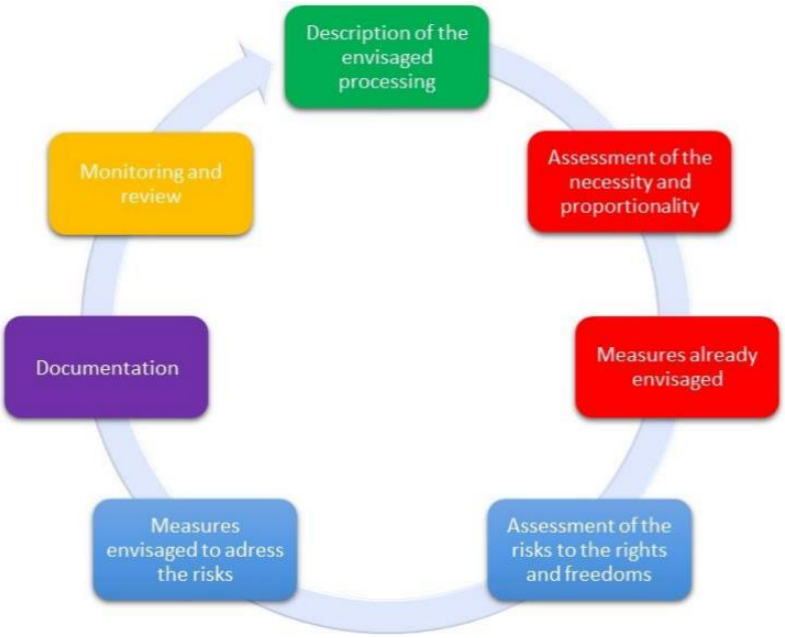
A DPIA is **not required** where the processing operations are based on a legal obligation or the performance of a public task, based on either EU or national law, provided that (i.) the law "regulates the **specific processing operation or set of operations in question"** and that (ii.) a DPIA has already been carried out "as part of the general impact assessment in the context of the adoption of that legal basis" (unless otherwise provided in the law) (Art. 35 (10) GDPR).

b) When shall the DPIA be conducted?

In principle, the DPIA shall be conducted **prior to** the envisaged data processing in question. The DPIA is therefore inevitably conducted, to some extent, in the abstract. A single assessment may address **a set of similar processing operations** that present "similar high risks" (Art. 35 (1) GDPR) or, alternatively, for a single operation.

[94] Article 35(3) of the GDPR.
[95] Article 35(4) of the GDPR.
[96] For instance, the French supervisory authority (CNIL) issued both a list of data processing activities which do require a prior DPIA and a list of data processing activities which do not require a prior DPIA, https://www.cnil.fr/en/node/114419 (last visited 14th March 2020).
[97] Article 35(1) of the GDPR.

While a DPIA is not required for **existing processing operations** (which started before the entry into force of the GDPR) **in principle,** it shall be required in case where there has been a change of the risks, taking into account the nature, scope, context and purposes of the processing, particularly where the



supervisory authority did not check the operations.

Both the DPIA and the processing operations that it assesses **shall be periodically reviewed**, at least when there is a change of the risk posed by the processing operations (Art. 35 (11) GDPR and WP29 Guidelines). The change of the risk is especially expected to stem from either a change in the processing operations (e.g. new technologies, broadened scope of the processing, etc.) or from a **change in the environment** (WP29). In other words, the DPIA shall be viewed as an iterative process – rather than as a "ex ante" obligation, as illustrated by the following figure issued by WP29.

Figure 3: A general process for carrying out the DPIA

Finally, a data protection impact assessment is one of the starting points for the controllers to apply the requirements of privacy by design to the actual technology.[98] A DPIA is carried out as a part of the design phase.

c) What is a DPIA and what is it for?

The DPIA is essentially "a process for building and demonstrating compliance" (WP29). It detracts from the risk-based approach of the GDPR and from the principle of accountability. Because it is a tool for managing risks to the rights of the data subjects, it should therefore take **their** perspective, unlike risk management in other fields (e.g. information security where the focus is placed on the organization.[99] The GDPR does impose neither a specific form nor a given methodology to conduct the DPIA. It remains therefore up for the controller to choose a format and methodology, although the latter should genuinely enable the DPIA to comply with the GDPR requirements.

A DPIA shall contain at least the following components (Art. 35 (7) GDPR), as further specified in the DPIA Guidelines developed by the WP29:

i. **A systematic description** of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller. The description of the processing shall be **functional.** It shall define the expected recipients of the data as well as the duration for which data will be stored. Another requirement is **identification of the assets**, on which personal data rely, such as software, hardware, networks, people, paper or paper transmission channels.

ii. **An assessment of the necessity and proportionality of the processing operations in relation to the purposes**. The controller shall determine the measures envisaged to comply with the GDPR. On the one hand, measures **contributing** to the proportionality and the necessity of the processing shall be identified. On the other, measures contributing to the **rights of the data subjects** shall be identified (i.e. information provided to them, right of access, etc.).

iii. An **assessment of the risks to the rights and freedoms of data subjects**. The origin, nature, severity of the risks shall be appreciated (Rec. 84), with the assessment being required for each risk **from the perspective of the data subjects** (WP29).

[98] See Cavoukian, Ann. Privacy by design in law, practice and policy, 2011, p. 15, available at http://www.ontla.on.ca/library/repository/mon/25008/312239.pdf and ENISA, Privacy and Data protection by design, 2014, p. 12 and the following.

[99] This section is wholly based on: Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA), p. 21.

iv. The **measures envisaged to address the risks**, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned. Compliance with approved 'codes of conduct' (within the meaning of the GDPR) shall be taken into "due account" in assessing the impact of the processing operations, in particular for the purposes of a DPIA (Art. 35 (8) GDPR). According to WP29, compliance with approved codes of conduct can be useful to demonstrate that "adequate measures have been chosen or put in place", provided of course that the code of conduct is appropriate to the processing operation in question. In this respect, certification, seals and marks for the purpose of demonstrating compliance within the meaning of the GDPR (see Art. 42 GDPR), or 'Binding Corporate Rules' ('BCR') should also be taken into account (see also Rec. 77 GDPR).

Risk level (high or not) based on	Risk-based compliance obligation
categories of data (sensitive) (Recital 51, 53)	Personal data which are, by their nature, particularly **sensitive** in relation to fundamental rights and freedoms **merit specific protection** as the context of their processing could create significant risks to the fundamental rights and freedoms.
categories of data subjects (children) (Recital 38)	**Children merit specific protection**, as they may be less aware of the risks.
likelihood and severity the risk for rights and freedoms of natural persons	**The higher the risk, the stricter the compliance obligation:** ● the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures (Article 25) ● the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security (Article 32) ● the controller must notify the personal data breach to the supervisory authority (Article 33) ● the controller shall communicate the personal data breach to the data subject without undue delay (Article 34, Recital 86) ● DPIA (Article 35, Recital 84, 90, 91, 94) ● obligation to notify the processing of personal data to the supervisory authorities (Recital 89) ● obligation to keep records of processing activities (Article 30) ● data protection officer (Articles 37-39)

Table 1: Risk-based compliance

d) Involvement of interested parties

In order to protect legitimate interests of interested parties, the data controller must **seek the advice of the data protection officer** when carrying out the DPIA, as well as seek the views of data subjects or their representatives, if appropriate. This means consulting the representatives of employees as well as citizens, depending on the data processing operations. Such consultation is, however, inappropriate if it harms the protection of commercial or public interests or the security of processing operations.[100]

The controller is also required to **notify the competent supervisory authority** if the DPIA indicates that the processing would **result in a high risk in the absence of measures taken by the controller to mitigate such a risk**.[101] When doing so, the controller shall provide appropriate information, as laid down in Art. 36 (3) GDPR. If the supervisory authority considers such processing to be a potential infringement of the GDPR, especially if the controller has insufficiently identified or mitigated the risk, then the authority will provide written advice to the controller. It may also act according to Article 58 of the GDPR, which grants it investigative, corrective, authorisation and advisory powers.

6.9 What does the GDPR provide with respect to automated decisions?

The GDPR imposes an obligation on data controllers to implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

This obligation has a corresponding right for the data subject to contest such decisions. This right is, however, not applicable when the decision is:

i. necessary for entering into, or performance of, a contract between the data subject and a data controller,
ii. authorized by Union or Member States law or
iii. based on the data subject's explicit consent.

In both the first and the third case, the controller should implement the said **suitable measures.** Equally, Articles 13 (2) (f) and 14 (2) (g) GDPR require controllers to provide *meaningful information about the logic involved*, as well as the significance and the envisaged consequences of such automated decision-

[100] Article 35(9) of the GDPR.

[101] Article 36(1) of the GDPR.

making. Similarly, Article 15 (1) (h) GDPR prescribes that such information should also be provided to data subjects in the context of an access request.

The Article 29 Working Party's Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 clarify that **profiling and automated decision-making should not be equated.**[102] The guidelines specify that automated decision-making may be the result of profiling, but it has a different scope in the sense that such decision-making can be made with or without profiling and also that decisions which are not solely automated can include profiling.[103] Article 4(4) GDPR defines 'profiling' as "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*". **Profiling is thus: (1) an automated form of processing; (2) of personal data; (3) with the purpose of evaluating a natural person's personal aspects**.

The Article 29 Working Party identifies three ways in which profiling may be used, i.e.: (1) general profiling; (2) decision-making based on profiling; and (3) solely automated decision-making, including profiling, which produces legal effects or similarly significantly affects the data subject.

The provision of Article 22(1) GDPR has been interpreted by the Article 29 Working Party to mean a "general prohibition" of decision-making based solely on automated processing which applies regardless of whether the data subject has taken an action regarding the processing of their personal data.[104] In the Working Party's view, Article 22(2) provides for exceptions to the general prohibition which require that measures be placed to safeguard data subject's rights, freedoms and legitimate interests. The **general prohibition** applies whenever the following conditions have been met cumulatively:

i. The decision is based solely on automated processing, i.e. there is no human involvement in the decision process[105]
ii. The decision produces legal effects[106] or significantly affects the data subject[107]

[102] Article 29 Working Party, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (WP251rev.01), p. 8.
[103] Ibid.
[104] Ibid. 19.
[105] Ibid. 20.
[106] Article 29 Working Party provides the following examples: cancelation of a contract, refused admission to a country or denial of citizenship etc. See ibid. 21.
[107] According to Article 29 Working Party, such decisions must have the potential to "significantly affect the circumstances, behavior, or choices of the individual concerned", "have a prolonged or permanent impact on the data subject" or "at its most extreme, lead to exclusion or discrimination of individuals. The Working Party provides the following examples: decisions that affect someone's financial circumstances, such as their eligibility to credit, decisions that affect someone's access to health services etc. See ibid. 21-22.

In any case, data controllers must observe the data subject's rights. More specifically, they must comply with the requirements of Articles 13(2)(f) and 14(2)(g) GDPR regarding the right of the data subject to be informed. These requirements oblige data controllers to provide specific, easily accessible information about automated decision-making, based solely on automated processing, including profiling, that produces legal or similarly significant effects. This means that in any such case the controller must:[108]

i. Inform the data subject they are subject to such type of activities
ii. Provide "meaningful" information about the "logic" involved and
iii. Explain the significance and envisaged consequences of the processing.

There has been an extensive academic debate as to what the requirement to provide meaningful information about the logic involved entails. The Article 29 Working Party situates the debate in the context of the growing complexity of machine learning and the need of explainability and transparency of machine learning models. While the group clarifies that the explanation does not have to be a complex elaboration or disclosure of the algorithms used, it notes that the information must be "sufficiently comprehensive for the data subject to understand the reasons for the decision".[109] The explanation should also extend to cover the 'significance' and 'envisaged consequences' which could be made through examples of possible effects.

The Article 29 Working Party has identified some good practices which may be helpful in delivering this information to the data subjects, such as providing information on:

- Categories of data used or planned to be used in the decision-making
- Explanations regarding the relevance of these particular data
- Information on how the profile is built, including statistics used
- Information on why the profile is relevant to the decision-making process
- Information on how the profile is used to make a decision

Furthermore, controllers must implement suitable safeguards in the cases where an exception is applicable. The Article 29 Working Party highlights the importance of transparency and points out that such measures must provide means for the data subject to obtain human intervention, express their views and contest the decision. The Working Party advises controllers to perform regular assessments of the datasets in order to check for bias and to develop techniques to deal with "prejudicial elements" as well as methods for auditing of the models and testing procedures to prevent errors, inaccuracies or discrimination.[110]

[108] Ibid. 25.
[109] Ibid.
[110] Ibid. 27-28, 32.

In line with the accountability principle, Article 35(3)(a) GDPR provides that a **data protection impact assessment (DPIA)** is required in the case of systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. On this matter, see the 'DPIA' section.

6.10 What are the tasks of a Data Protection Officer (DPO)?

According to Art. 38 GDPR, the controller and the processor shall designate a data protection officer in the following cases:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

As provided in Art. 39 GDPR, the tasks of a DPO include the following:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
d) to cooperate with the supervisory authority;
e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The appointment of a DPO, acting as a contact point for both data subjects and supervisory authorities and in charge of the organisation's compliance with the GDPR, contributes to strengthening controllers' accountability.

As laid down in Art. 38(5) GDPR, the data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The controller and processor shall support the DPO and provide all the necessary resources for carrying out her tasks and shall restrain from providing any instructions regarding the performance of DPO's tasks (Art. 38(2)(3)).

7 Conclusions and Next Actions

Research ethics govern the standards of conduct for scientific researchers. It is important to adhere to ethical principles in order to protect the dignity, rights and welfare of research participants and to ensure quality research outcomes.

Ethics has a special place in H2020 projects. Responsible research and innovation is an approach that anticipates and assesses potential implications and societal expectations with regard to research and innovation, with the aim to foster the design of inclusive and sustainable research and innovation. The European Code of Conduct for Research Integrity is a steering document which offers a set of principles and priorities for self-regulation of the research community. It states four ethical principles TRUSTS should comply with: (i) Reliability in ensuring the quality of research, reflected in the design, the methodology, the analysis and the use of resources; (ii) Honesty in developing, undertaking, reviewing, reporting and communicating research in a transparent, fair, full and unbiased way; (iii) Respect for colleagues, research participants, society, ecosystems, cultural heritage and their environment; (iv) Accountability for the research from idea to publication, for its management and organisation, for training, supervision and mentoring and for its wider impacts.

The processing of personal data across national borders by both public and the private sector has increased exponentially in recent years, as has the need for legal protections for personal data. The legal instruments vary from the international treaties such as the European Convention of Human Right, the Council of Europe's Convention 108 and 108+ and the Budapest Convention; to European and national legal frameworks. The aim of the EU data protection law has traditionally been to facilitate the free flow of data within the EU under common standards for lawful processing, while safeguarding the fundamental rights of individuals. The GDPR sets down six principles for collection, use, sharing and storage of personal information data processing: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity, confidentiality and accountability.

Under the GDPR, the role of research is understood to provide knowledge that can in turn improve the quality of life for a number of people and improve the efficiency of social services. The GDPR assumes a broad definition of "research" and applies a special regime for scientific research which permits some derogations from controller obligations. This includes the presumption of compatibility of processing for scientific research purposes of data collected in commercial and other contexts, provided appropriate safeguards are in place.

Privacy and data protection in the context of AI means that AI systems should be designed to guarantee privacy and data protection of its users. To this end, AI developers should apply design techniques such as data anonymization and they should ensure the quality of the data.

The AI brings many benefits, they also highlight a number of ethical concerns, relating primarily to the risks facing human rights and fundamental freedoms. Therefore, we shed some light on the ethical rules that are now recommended by the AI HLEG and OECD when designing, developing, deploying, implementing or using AI products and services in the EU and beyond. As the legislative framework around the AI develops, more in-depth analysis of the AI ethical and legal framework in the context of TRUSTS will be needed.

It is important to underline that compliance with ethics and legal requirements are considered a continued effort by the partners, to be maintained throughout the project.

The work performed in this task will serve as a basis for our further work in the TRUSTS project. In particular, in task T6.3 KUL, in close collaboration with the technical partners responsible for defining the platform architecture and developing the platform technologies, will guide and assess the integration of the legal and ethical requirements in the design of the platform. As the technical development of the project evolves, the task will:

- provide oversight and guidance on the implementation of the legal and ethical requirements;
- provide clarification on legal and ethical issues that may arise;
- potentially identify legal and ethical barriers based on the research conducted in T6.3;
- keep the partners updated with regards to future legal developments that are relevant to the project;

  This will include in particular analysis of the upcoming initiatives in the field of online platforms (e.g. Digital Services Act), data governance (such as Data Governance Act and Data Act), privacy (ePrivacy Regulation) and in the field of AI, including the Updated Coordinated Plan on AI and the European Commission Legislative proposal on AI – both planned for first quarter 2021.

  Also, in its guidelines (currently in preparation and due in 2021) on the processing personal data for scientific research purposes, the EDPB will elaborate further on these issues while also aiming to provide a more comprehensive interpretation of the various provisions in the GDPR that are relevant for the processing of personal data for scientific research purposes.

- validate the project from the legal and ethical point of view.

The task will result in Deliverable D6.3 Legal and Ethical Assessment. In Deliverable D6.4 we will build upon the previous work packages in order to point out the potential legal gaps and barriers identified and the lessons learned in the course of the project. It will thus lead to tailor made recommendations regarding the employment of the platform in compliance with the established legal rules and ethical principles. The task will result in Deliverable D6.4 Legal and Policy Recommendations.

Annex I: Questions to partners - Ethics requirements with respect to personal data

Introduction - context

The present questionnaire is aimed at ensuring that data protection law and applicable ethics requirements are complied with throughout the research project, with respect to the personal data processing activities taking place. The questionnaire is circulated amongst the project partners involved in each use case ('purpose', within the meaning of data protection law). Based on the information gathered, tailored legal and ethics guidelines will be provided in order to ensure compliance. The questionnaire is accompanied by a background note, which provides further explanation to facilitate the filling in of the questionnaire. Please note that the background note does not provide an exhaustive overview of the GDPR provisions and obligations.

The questionnaire - together with the background note - and the ensuing legal and ethics requirements follow an **iterative process**, in order to best guide partners into compliance.

For this reason, a note needs to be made:

- **It is ok to have doubts** as many aspects of personal data protection are not straightforward and much context-specific (e.g. whether such data is 'personal data' or not);
- **It is also ok not to be able to answer *yet*,** as some aspects will depend and change during the project.

It is however **crucial to document doubts or remaining open questions, as early as possible, while filling in the questionnaire**, in order for WP9 to provide support and guidance in this regard.

Finally, answers can be provided in any form and format and do not have to fit in the table (e.g. figures or Gantt charts can be provided).

1. The basics: purpose for processing personal data

Question	Answer
What is(are) the use case / purpose(s)? What is the reference in the proposal / GA? How do you ensure that you do not process/collect more personal data than necessary	

for the project purposes? If the data processing is necessary to comply with a legal obligation under national law, please indicate relevant legal acts.	
Which personal data (categories) are processed or will be processed? If it is not (yet) possible to identify which personal data (categories) will be processed, explain why. Could you achieve the same purpose with 'less' personal data - or data less sensitive -? If you don't know (yet), please explain. Is there a need for a declaration on compliance and/or authorisation under your national law for processing (special categories of) personal data?	
What will you do with the collected personal data after the end of the project? If stored, where, for how long and what safeguards are deployed? Please document if you are not (yet) in a position to answer.	

2. The data subject(s)

Question	Answer
Who are the data subjects (natural persons to whom the data relate) - or what are the	

categories of data subjects? If you don't know (yet), please document.	
Do you interact with the natural persons to whom the data relate at some point, and why? E.g. Do you collect the data directly from them?	
What consequence(s) - both beneficial and detrimental - do you anticipate the data processing activities could have on the data subjects (the natural persons to whom data relate)? If you don't know (yet), please explain why.	

3. The data processing activities: what is done with the data

Question	Answer
What is the workflow of the data processing activities? Please describe the various steps.	
According to you, is there some point in the process where data should no longer be considered "personal" (e.g. following anonymisation)?	
How do you collect the data and from which source(s)? Do you have a relationship with such entity(ies) (e.g. a	

contract) - or do you intend to have one?	
Do you use machine-learning techniques, 'AI' or other forms of data processing automation and if so how and why?	

4. How are the data being protected? Technical and organizational aspects

Question	Answer
How do you intend to ensure that data are 'accurate'? If not possible, please explain.	
Where and for how long do you store the personal data? Are the data stored at your premises? Are they entrusted to a subcontractor? Please explain.	
Which technical and organisational measures do you envisage to protect the confidentiality ('must-know' basis) and security of personal data?	
Do you envisage 'privacy by design' measures, and, if so, for what concrete purpose(s)?	
Do you have a DPO?	

5. Profiling and automated decision-making

Question	Answer
Do you perform any profiling activities? What is their impact on fundamental rights of data subjects? How do you inform data subjects about possible profiling activities?	
How do you avoid algorithmic bias? (Describe the envisaged measures). How do you avoid other potential detrimental impact on individuals rights and freedoms?	
Please provide information on the Artificial Intelligence/ Data Mining system and related decision making procedures, including human actors' roles and responsibilities.	

Annex II: Template of informed consent (data processing)[111]

By signing this form you agree to the processing of your personal data for research purposes within the TRUSTS project. **Your participation is voluntary and your consent can be freely withdrawn at any time** (Art. 7 (3) GDPR).

1. **What is TRUSTS?**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 871481 and will last 3 years until the 31 December 2022.

TRUSTS is a consortium of partners who together conduct research. TRUSTS partners are the following entities:

- DATA INTELLIGENCE OFFENSIVE
- EBOS TECHNOLOGIES LIMITED
- ELLINIKI ETAIRIA TILEPIKOINONION KAI TILEMATIKON EFARMOGON AE
- EMC ISRAEL ADVANCED INFORMATION TECHNOLOGIES LTD
- FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
- GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER => Coordinator
- GOVERNANCE ONE GMBH
- IDRYMA TECHNOLOGIAS KAI EREVNAS
- INTERNATIONAL DATA SPACES EV
- KU Leuven CiTiP
- KNOW-CENTER GMBH RESEARCH CENTER FOR DATA-DRIVEN BUSINESS & BIG DATA ANALYTICS
- LSTECH ESPANA SL
- RELATIONAL ROMANIA SRL
- RESEARCH STUDIOS AUSTRIA FORSCHUNGSGESELLSCHAFT MBH
- SEMANTIC WEB COMPANY GMBH
- TECHNISCHE UNIVERSITEIT DELFT
- TRAPEZA PEIRAIOS AE

2. **Purposes of data processing**

The purpose of the TRUSTS research project is the development and testing of a federated data marketplace.

Since TRUSTS is a research project, we are conducting a number of pilot testing:

[111] This consent form will be translated in all the relevant languages, where appropriate.

Use case 1: The AML Services that will be used through the TRUSTS Platform by the providers FNET & InBestMe (or other Financial Institutions). As part of this project, we will leverage the power of the TRUSTS Platform in view of securely sharing data between organisations, applying smart big data analytics for AML compliance purposes as well as fairly trading the resulting data to end-users such as FIs, internal / external auditors, fiduciaries, audit firms, etc.

Use case 2: The purpose is to verify that TRUSTS services can be used to advance current marketing activities extending towards enabling collaboration between different enterprises in a GDPR complaint manner.

Use case 3: Automation of debt management: the data acquisition to improve customer support services use case. The TRUSTS Data Marketplace vision is to create an out-of-the-box analytics solution for the anonymization and visualization of Big Financial Data, specifically to advance new ways of human-computer interaction currently in their infancy, e.g. chatbots that can act as automated assistants to allow customers to converse about the management of their debt at their own pace and with a personalized experience, through the integration of Big Data.

None of the personal data acquired will be disseminated or distributed outside the TRUSTS consortium. More information with regard to the TRUSTS research policy can be obtained from the project coordinator:

Alexandra Garatzogianni - H2020 Coordinator of TRUSTS Trusted Secure Data Sharing Space, Senior Project Manager, Leibniz University of Hannover, L3S Research Center & Head of Tech Transfer, EU-Project Coordination & Management, Leibniz Information Center for Science and Technology, University Library

3. The type of data that will be processed

Subject to your consent, the following categories of personal data will be processed (indicate at the moment of data collection).

4. Who gets access to my data?

No personal data will be shared with third parties, namely beyond the TRUSTS partners. The results of the research, which will be made available, will not contain any personal data.

TRUSTS partners will get access to the data, subject to ‘use case-based access’ and ‘must-know’ principle throughout the project. If a partner does not need to access data for the purpose of the research, then no access should be granted to him/her.

5. Will my data be transferred to third countries outside the European Union?

No personal data will be transferred outside the European Union to third countries.

6. Is my data secure?

To the extent possible, yes. We do everything in our capacity to ensure that the confidentiality over the personal data we processed is protected. This means, inter alia, applying the following measures:

- Anonymization techniques as described in D9.6.
- Access control and authentication-based environments are applied to the access to data-sets containing personal data
- Need-to-know principle is implemented in the vetting of any researcher involved in TRUSTS personal data processing operation.

7. For how long will you retain my data?

If immediate deletion will not occur, that means we have a legal obligation and/or a research purpose to archive the data either for contractual reasons or for scientific research finalities. If required, we may retain the information for a year after the termination of the project. By then, personal data will be deleted. We will apply anonymization and minimization techniques in order to minimize any risk of confidentiality breach or unintentional data breach.

8. What principles will you apply when processing my personal data?

- Accountability. We maintain and regularly update internal policies enabling the consortium to keep records and documentation of the relevant personal data processing operations.
- Awareness raising. We regularly undertake activities aimed at informing our consortium partners about the data protection obligations and standards that we abide to.
- Ethical standards. As said above, we do not only regard the protection of personal data and privacy as a legal requirement to meet. TRUSTS project considers personal data protection obligations as an ethical standard of best practice.

9. What are my rights?

- Right to access. You are entitled to request information regarding your personal data, including purposes, categories of information, recipients, retention, source of collection, transfer to third-countries (non-EU Member States). Moreover, the data subject is entitled to receive a copy of such data.

- Right of erasure or rectification. You may request at any time for your personal data to be amended, updated or erased by the controller. If the personal data has been anonymized, it will be impossible to destroy the data.

- You have the right to lodge a complaint against TRUSTS regarding data protection issues with any data protection authority within the European Union (Article 13(2)(d) GDPR).

- Restriction of processing. You have the right to request that your data are suspended from being processed, if the data are inaccurate or unlawfully or unnecessarily processed.
- Object. You have the right to object to the processing of your personal data, unless the processing is conducted on public interest grounds

10. Where can I find more information?

- **Visit our website and our social media**. You can have a good understanding of what we do by visiting our public website, our Twitter account or our LinkedIn account.
- **Consult the GDPR**. Our main legal framework is the GDPR – General Data Protection Regulation. Have a look at it and at Article 89, which establishes minimum rules and procedures for privacy protection in the research domain.
- **Ask us!** If you're reading this notice, this means that one of us is there with you. We are more than happy to answer all questions you may have or, eventually, address you to our legal people.

Declaration of consent to the processing of personal data:

I accept that, I have read and agree with the TRUSTS data protection policy as they are described below:

- The data I provide will be used only for research purposes.
- The data I provide may be published internally or externally and be used as part of presentations related to the research.
- I may withdraw my consent to the processing of personal data at any moment.

If you have any questions about the research after you sign this document, you can contact the research team using the information provided above.

I have read and understand the conditions and consent to processing of my personal data as described.

Name: _____

Signature: _____

Date of Signature (mm/dd/yy): _____

Annex III: Consent form template (questionnaires, workshops, focus groups)

You are invited to take part in the TRUSTS project questionnaire/workshop. Your participation is voluntary and you may decide to withdraw it at any time.

The purpose of the TRUSTS research project is the development and testing of a federated data marketplace. This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No 871481 and will last 3 years until the 31 December 2022.

TRUSTS is a consortium of partners who together conduct research. TRUSTS partners are the following entities:

- DATA INTELLIGENCE OFFENSIVE
- EBOS TECHNOLOGIES LIMITED
- ELLINIKI ETAIRIA TILEPIKOINONION KAI TILEMATIKON EFARMOGON AE
- EMC ISRAEL ADVANCED INFORMATION TECHNOLOGIES LTD
- FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
- GOTTFRIED WILHELM LEIBNIZ UNIVERSITAET HANNOVER => Coordinator
- GOVERNANCE ONE GMBH
- IDRYMA TECHNOLOGIAS KAI EREVNAS
- INTERNATIONAL DATA SPACES EV
- KU Leuven CiTiP
- KNOW-CENTER GMBH RESEARCH CENTER FOR DATA-DRIVEN BUSINESS & BIG DATA ANALYTICS
- LSTECH ESPANA SL
- RELATIONAL ROMANIA SRL
- RESEARCH STUDIOS AUSTRIA FORSCHUNGSGESELLSCHAFT MBH
- SEMANTIC WEB COMPANY GMBH
- TECHNISCHE UNIVERSITEIT DELFT
- TRAPEZA PEIRAIOS AE

The TRUSTS consortium aims at receiving responses to the questionnaire and interviewing industrial, academia and regulatory domain experts in order to lead the TRUST data marketplace specification. Your responses will help us to evaluate the functionality, services and operational capacity of such an endeavour and to establish its operation.

None of the personal data acquired will be disseminated or distributed outside the TRUSTS consortium.

More information with regard to the TRUSTS research policy can be obtained from the project coordinator:

Alexandra Garatzogianni - H2020 Coordinator of TRUSTS Trusted Secure Data Sharing Space, Senior Project Manager, Leibniz University of Hannover, L3S Research Center & Head of Tech Transfer, EU-

Project Coordination & Management, Leibniz Information Center for Science and Technology, University Library

Declaration of consent to participate in the research questionnaire:

By agreeing to answer this questionnaire I accept that, I have read and agree with the project pilot participation rules and regulations as they are described below:

- This survey is being performed as part of a research project.
- The data I provide will be used only for research purposes.
- The data I provide may be published internally or externally and be used as part of presentations related to the research. Any publication of the data will be in an anonymised form with all identifying personal information removed.
- I may withdraw my consent to participate in this research questionnaire and to the processing of personal data at any moment.
- Personal data provided are limited to the identification of the respondent (name/title) and to their place of employment. Such information are processed based on the legitimate interest of the TRUSTS consortium, namely to conduct scientific research as described in the document.

Your rights:

- Right to access. You are entitled to request information regarding your personal data, including purposes, categories of information, recipients, retention, source of collection, transfer to third-countries (non-EU Member States). Moreover, the data subject is entitled to receive a copy of such data.

- Right of erasure or rectification. You may request at any time for your personal data to be amended, updated or erased by the controller. If the personal data has been anonymized, it will be impossible to destroy the data.

- You have the right to lodge a complaint against TRUSTS regarding data protection issues with any data protection authority within the European Union (Article 13(2)(d) GDPR).

- Restriction of processing. You have the right to request that your data are suspended from being processed, if the data are inaccurate or unlawfully or unnecessarily processed.

- Object. You have the right to object to the processing of your personal data, unless the processing is conducted on public interest grounds

If you have any questions about the research after you sign this document, you can contact the research team using the information provided above.

I have read and understand the conditions and consent to processing of my personal data as described.

Name: _____

Signature: _____

Date of Signature (mm/dd/yy): _____