



Co-funded by
the European Union

“Advanced Digital Skills on Blockchain for Trusted Food Supply Chains”

*Project: 101100804 — TRUST-FOOD
DIGITAL-2022-TRAINING-02-SHORT-COURSES*

Deliverable: 1.2

Ethics dimension in research content

Work Package 1

Responsible Partner: REZOS BRANDS



This project has received funding from the European Union's Digital Europe Programme under Grant Agreement N° 101100804

D1.2: Ethics dimension in research content

Issued by:	REZOS BRANDS
Issue date:	13/11/2023
Due date:	31/12/2023
Work Package Leader:	REZOS BRANDS

Start date of project: 01 January 2023

Duration: 36 months

Document History		
Version	Date	Changes
0.1	11/12/2023	Initial Version
0.2	12/12/2023	Draft version that includes UNIC's input
0.3	27/12/2023	Final version that includes AUA's input

Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the EC Services)	
RE	Restricted to a group specified by the consortium (including the EC Services)	
CO	Confidential, only for members of the consortium (including the EC)	

Main authors	
Name	Organisation
Anastasia Vlachou	Rezos Brands
Dimitrios Tsolis	Rezos Brands

Quality reviewers	
Name	Organisation
Marianna Charalambous	UNIC
Sotirios Karetsos, Konstantinos Demestichas	AUA

LEGAL NOTICE

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

© TrustFood Consortium, 2023

Reproduction is authorised provided the source is acknowledged.

Contents

Executive Summary	7
1. Introduction.....	8
2. Legal & Ethical Framework	10
2.1. Overview.....	10
2.2. International Conventions.....	10
2.2.1. The European Convention of Human Rights	11
2.2.2. The Council of Europe’s Convention 108 on Personal Data	11
2.2.3. The Council of Europe’s Convention 108+ on Personal Data	13
2.2.4. The Budapest Convention – Cybercrime Convention – Convention 185	13
2.3. European Union Primary Legislation	14
2.3.1. Overview.....	14
2.3.2. The Charter of Fundamental Rights of the European Union	14
2.3.3. The Treaty of the European Union and the Treaty on the Functioning of the European Union	16
2.4. Secondary European Union Legislation.....	16
2.4.1. Overview.....	16
2.4.2. The General Data Protection Regulation.....	17
2.4.2.1. Background and scope of the General Data Protection Regulation.....	17
2.4.2.2. Key Definitions.....	17
2.4.2.3. Key Regulatory Points of the General Data Protection Regulation	18
Data Protection Principles	18
Data Security	18
The Rights of the Data Subject	19
Consent.....	19
2.4.3. ePrivacy Directive	20
2.4.4. The ePrivacy Regulation	20
2.4.5 Ensuring compliance with the General Data Protection Regulation principles within the TRUST-FOOD project	20

3.	TRUST – FOOD – Ethics	22
3.1.	General Information	22
3.1.1.	Grant Agreement – Ethics – General Requirements	22
3.1.2.	Annex 5 of the TRUST – FOOD Grant Agreement.....	22
3.1.2.1.	CONFIDENTIALITY AND SECURITY (— ARTICLE 13).....	22
	Sensitive information with security recommendation.....	22
	EU classified information.....	23
3.1.2.2.	ETHICS (— ARTICLE 14).....	23
	Ethics.....	23
3.1.2.3.	INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE (— ARTICLE 16)	24
	Definitions	24
	List of background — Background free from restrictions	24
	Results free from restrictions	24
	Ownership of results	25
	Protection of results	25
	Exploitation of results.....	25
	Transfers and licensing of results	25
	Access rights — Additional rights of use	26
3.1.3.	Grant Agreement – Ethics – Task 1.3 – Ethics Management.....	27
3.1.4.	Consortium Agreement – Ethics.....	29
3.1.4.1.	Article 4, Section 4.4. Specific responsibilities regarding data protection	29
3.1.4.2.	TRUST – FOOD Project Ethics Committee	29
3.2.	Transfer and Use of Personal Data	29
3.3.	Non-EU Countries	30
4.	References	31

List of Figures

Figure 1: TRUST – FOOD Project’s Specific Objectives	8
Figure 2: Moral Virtues	10
Figure 3: Basic principles of Data Protection – Article 5 of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	12
Figure 4: Human Rights protected by the Charter of Fundamental Rights of the EU	15
Figure 5: The seven protection and accountability principles.....	18
Figure 6: The Rights of the Data Subject according to the General Data Protection Regulation (GDPR)	19
Figure 7: The Ethics Committee’s Chairperson and members in the TRUST – FOOD project.....	27
Figure 8: The Ethics Deliverable in the TRUST – FOOD project	28

Executive Summary

Deliverable 1.2 provides an overview of the legal and ethical framework surrounding data protection and privacy in the European Union and internationally. It covers international conventions such as the European Convention of Human Rights and the Budapest Convention, as well as EU primary and secondary legislation including the General Data Protection Regulation and the ePrivacy Directive. The deliverable also presents the ethical requirements and considerations related to the TRUST – FOOD project, including confidentiality and security, ethics management, and intellectual property rights. Finally, it addresses the transfer and use of personal data and the implications for non-EU countries.

1. Introduction

The project “**TRUST – FOOD: Advanced Digital Skills on Blockchain for Trusted Food Supply Chains**” (G.A. **101100804**) has been approved for funding by the **Digital Europe Programme (DIGITAL)**, a new EU funding programme focusing on bringing digital technology to businesses, citizens and public administrations.

TRUST-FOOD overarching objectives (Figure 1) is to address the capacity development-related challenge of Blockchain adoption across the agrifood sector, by designing and delivering short-term training courses in Blockchain Technologies (BCT), for upskilling and reskilling of the labour force, with a particular focus on SMEs owners, managers, and employees in the Food Supply Chain (FSC). The courses will be highly practical and will provide specific knowledge about key digital technologies of Blockchain and their applications to the FSC. To reach this general objective, the following specific objectives should be successfully addressed:

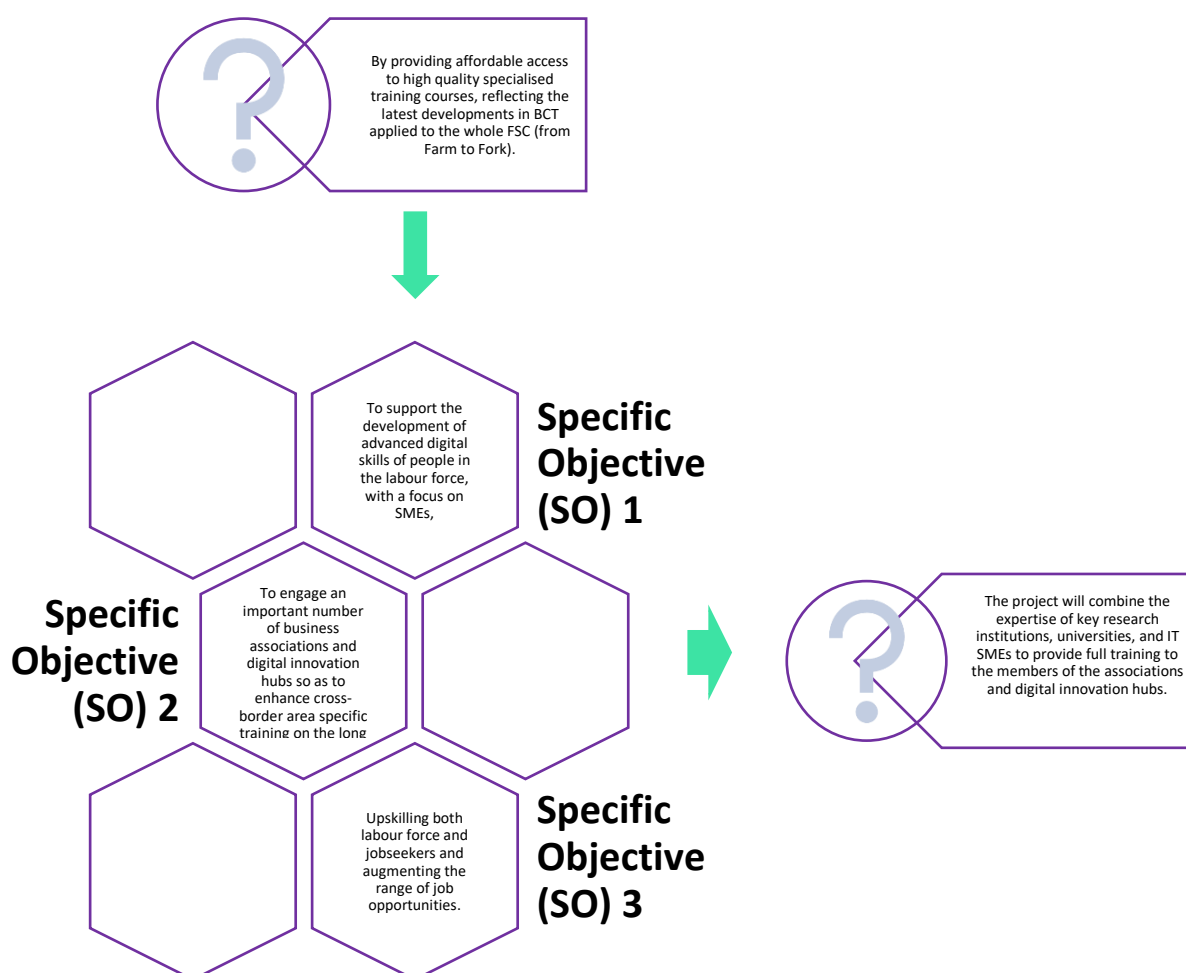


Figure 1: TRUST – FOOD Project's Specific Objectives

TRUST-FOOD consortium, led by Rezos Brands, is comprised of 5 SMEs, 3 Universities, 3 agrifood associations, 3 European Digital Innovation Hubs (EDIH), and 1 Living Lab (LL). It is built with members who can guarantee the delivery of blockchain short courses tailored to the needs of agrifood SMEs. Training activities are being carefully designed, based on the agrifood-specific expertise of the business associations partners, to ensure that they are relevant for the agri-food workforce, meet the needs of the labour market and address existing BCT skills shortage. The educational material and training are elaborated by the education (Universities) and training providers (training SMEs) of the consortium, who are experts in the fields of BCT, agrifood, and adult training. Agrifood SMEs already adopting BCT bring to the consortium valuable professional insights and validate the final content of the courses. The EDIHs and the LL act as intermediaries between SMEs and universities/training providers at the local level, as a gateway to innovation good practices for the support of SMEs and entrepreneurship, and as a catalyst of information on opportunities, latest trends and insights on innovation.

2. Legal & Ethical Framework

2.1. Overview

When implementing a European project, the establishment of a legal framework and ethics principles are crucial. Adherence to ethical principles promotes respect of human rights and fair practices, while compliance with a legal framework ensures legality and consistency. In addition to maintaining trust among stakeholders, European projects can contribute to the advancement of European society overall by adhering to these principles and guidelines.



Figure 2: Moral Virtues

It is the principles and values that guide individuals and organizations involved in these projects when it comes to ethics. Keeping fairness, trust, and respect among all stakeholders is essential in a diverse and multi-cultural context such as Europe.

In terms of the legal framework, European projects need to comply with applicable laws and regulations both at the national level and at the European Union (EU) level. In order to ensure the legality, fairness, and consistency of these projects, a legal framework provides a set of rules and standards.

2.2. International Conventions

The EU ethics legislation consists of laws and regulations adopted by member states for the purpose of establishing and maintaining ethical standards in various sectors. Among other issues this legislation ensures that ethical principles are followed in various areas including research, healthcare, environmental protection, consumer rights, and business practices.

An integral part of EU ethics legislation is the promotion of responsible research and innovation. The EU has developed guidelines and frameworks to assist researchers and innovators in conducting their work ethically. The objectives include ensuring that all human and animal rights are treated in accordance with strict ethical

standards, protecting the privacy and personal information of those involved in research studies, and ensuring that participants are given their free and informed consent.

2.2.1. The European Convention of Human Rights

An international treaty established in 1950 by the Council of Europe, [The European Convention of Human Rights \(ECHR\)](#) provides protection and promotion of human rights across Europe. It is intended to ensure that individuals are able to live a dignified and fulfilling life by providing a range of fundamental rights and freedoms.

The convention protects several civil and political rights, including the right to life, freedom of expression, freedom of religion, and the right to a fair trial, which are among the key provisions of the ECHR. As a result of the ECHR, individuals are guaranteed fair and just treatment by their governments through the upholding of these rights.

An important aspect of the ECHR is the creation of the European Court of Human Rights (ECtHR). It is the responsibility of this court, located in Strasbourg, France, to hear complaints against individuals as well as governments that violate the convention. As a crucial body in enforcing the principles and values enshrined in the ECHR, the ECtHR has the power to influence national legislation and policies through its decisions.

A significant part of the ECHR's role has been to shape human rights laws and policies in Europe. It has promoted equality, challenged discrimination, and maintained the rule of law by promoting these principles. There are 47 member countries of the Council of Europe that have ratified the convention, demonstrating their commitment to ensuring human rights are protected and respected.

In the context of the TRUST FOOD project, Article 8 of the ECHR, stating that every individual is entitled to respect for his or her private and family life, home, and correspondence, is applied. Such a provision is essential to safeguarding the personal privacy and autonomy of an individual.

2.2.2. The Council of Europe's Convention 108 on Personal Data

[The Council of Europe's Convention 108 on Personal Data](#) is an international agreement aimed at protecting individuals' rights in relation to the processing of their personal data. It was adopted in 1981 and has since been ratified by numerous countries.

As part of the convention, principles and guidelines are outlined for the collection, storage, and processing of personal data. This convention emphasizes the need to maintain a balance between personal privacy rights and the need for organizations to utilize personal data in a legitimate manner.

There are several key objectives of Convention 108, including the establishment of a framework for the cross-border transfer of personal data. It promotes cooperation between member states to ensure that sensitive personal information is adequately protected during the process of transfer.

To comply with the convention, member states are required to establish a supervisory authority to oversee the implementation of data protection laws. These authorities are responsible for ensuring that organizations

comply with the principles set out in the convention and have the power to investigate complaints and impose sanctions for non-compliance.

Convention 108 was modernized through a Protocol in 2018 ([Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data \(ETS No. 108\)](#)), which formed the foundation of several data protection legal frameworks. This instrument imposes obligations for the signatories to ensure that appropriate safeguards are implemented in national law. It is worthwhile to illustrate the basic principles of data protection contained in Art. 5, which include (a) Lawful and fair processing, (b) purpose limitation, and (c) data quality and accuracy, (Figure 3).

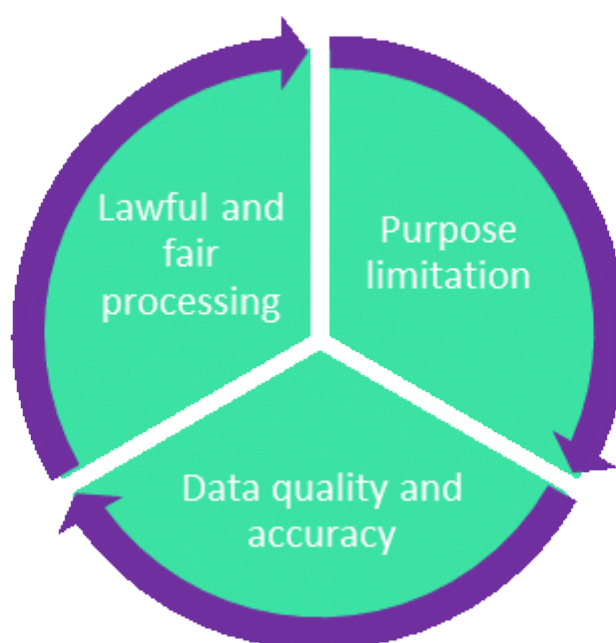


Figure 3: Basic principles of Data Protection – Article 5 of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

In addition to laying the foundation for modern data protection instruments, the Convention introduced the distinction between personal and sensitive data. Mentioning the sensitive data in Art. 6 of the Convention should suffice here, as sensitive data refers to data that indicates a person's racial origin, political opinions, religious or other beliefs, as well as health or sexuality.

Additionally, the Convention introduced rights for data subjects. More particularly, Article 8 of the Convention establishes the rights to information and to rectification or erasure.

It is well established that Convention 108 has a significant role in the jurisprudence of the ECtHR and is referred to as guidance in assessing the scope of the aforementioned Article 8 ECHR.

2.2.3. The Council of Europe's Convention 108+ on Personal Data

While the core principles that consist the Convention 108 have stood the test of time and its technologically-neutral, principle-based approach constitutes an undeniable strength, the Council of Europe decided that it was necessary to modernise its landmark instrument. This resulted in an updated version of the document, namely the Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, also known as the [Convention 108+](#).

Convention 108 was modernized with two main objectives in mind: to deal with the challenges arising from the use of new technology and to improve the effectiveness of the Convention's implementation.

As part of the Convention 108+, the following novelties have been added. In Art. 6, biometric data are explicitly included as special personal data, which has been updated. Secondly, Art. 9 specifies that data subjects do not have to be subject to a decision significantly affecting them solely because of automated processing without having their views taken into consideration. The consequence of this is that technology providers need to specify transparent and explicable processes when developing tools like big data analysis tools or machine learning algorithms.

2.2.4. The Budapest Convention – Cybercrime Convention – Convention 185

The Convention on Cybercrime also known as The Budapest Convention or Convention 185, opened for signature in Budapest, Hungary, in November 2001, is considered the most relevant international agreement on cybercrime and electronic evidence.

In addition to providing a framework for countries to work together to investigate and prosecute cybercrime, the Convention also establishes legal measures and procedures to address computer-related fraud, child pornography, and hacking.

One of the key aspects of the Budapest Convention is international cooperation. It encourages member states to collaborate by exchanging information, providing mutual legal assistance, and extraditing offenders, among other forms of cooperation. This is crucial in a digital world where cybercrimes can easily cross borders.

As part of the Convention, human rights and privacy are also protected. Participating countries are required to comply with international human rights standards in their legislation and actions. In this way, a balance can be struck between combating cybercrime and protecting individual rights while protecting privacy.

The Convention is supplemented by a [First Additional Protocol](#) covering the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS 189) and a [Second Additional Protocol on enhanced international co-operation and disclosure of electronic evidence \(CETS 224\)](#).

It is important to note however, that not all countries have ratified or signed the Budapest Convention. Several people are concerned about the Convention's impact on civil liberties, while others claim its provisions might infringe upon national sovereignty. However, the Convention has nonetheless been a major contribution to international cooperation in combating cybercrime and promoting safer digital

environments. By September 2023, 68 States were Parties to the Convention (European countries as well as Argentina, Australia, Brazil, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ghana, Israel, Japan, Mauritius, Morocco, Nigeria, Panama, Paraguay, Peru, Philippines, Sri Lanka, Senegal, Tonga and the USA), an additional 2 countries had signed it (Ireland and South Africa), and 19 countries had been invited to accede (Benin, Burkina Faso, Cameroon, Côte d'Ivoire, Ecuador, Fiji, Guatemala, Kazakhstan, Kiribati, Korea, Mexico, New Zealand, Niger, Sierra Leone, Timor-Leste, Trinidad and Tobago, Tunisia, Uruguay and Vanuatu). These 89 States participate as members (Parties) or observers (signatories or invitees) in the [Cybercrime Convention Committee \(T-CY\)](#) .

2.3. European Union Primary Legislation

2.3.1. Overview

The laws and regulations directly adopted by the EU are defined as the Primary EU legislation. These laws, binding on all EU member states, have the highest legal authority within the EU legal system.

The primary EU legislation for ethics is vast and constantly evolving, with new laws and regulations being introduced to address emerging ethical issues. It refers to those laws and regulations that govern ethical standards and behaviours within the EU.

The EU operates under the framework of international treaties that promote ethical values and cooperation in various domains. One of the most prominent pieces of primary EU legislation regarding ethics is the Treaty on European Union (TEU), also known as the Maastricht Treaty. Moreover, The Treaty on the Functioning of the European Union (TFEU) serves as the foundation for the EU's external action, especially in areas such as development cooperation, human rights, and trade. One more yet crucial document pertaining to ethics within the EU is the Charter of Fundamental Rights of the EU.

2.3.2. The Charter of Fundamental Rights of the European Union

The [Charter of Fundamental Rights of the EU](#) a crucial document that outlines the fundamental rights and freedoms guaranteed to all individuals within the EU. It was first proclaimed in 2000 and has since been legally binding with the entry into force of the Lisbon Treaty in 2009.

This Charter aims to protect the rights of EU citizens by establishing a clear set of principles that all Member States must adhere to. It covers various aspects of human rights, consisting of general provisions, dignity, freedoms, equality, solidarity, citizen's rights, and justice (Figure 4). The Charter recognizes economic, social, and cultural rights, such as the right to work, fair working conditions, healthcare, education, and social protection. Furthermore, the Charter promotes the principles of transparency, accountability and democracy within the EU institutions. It guarantees the right to participation in public affairs, freedom of expression, and the right to access documents held by the EU institutions.

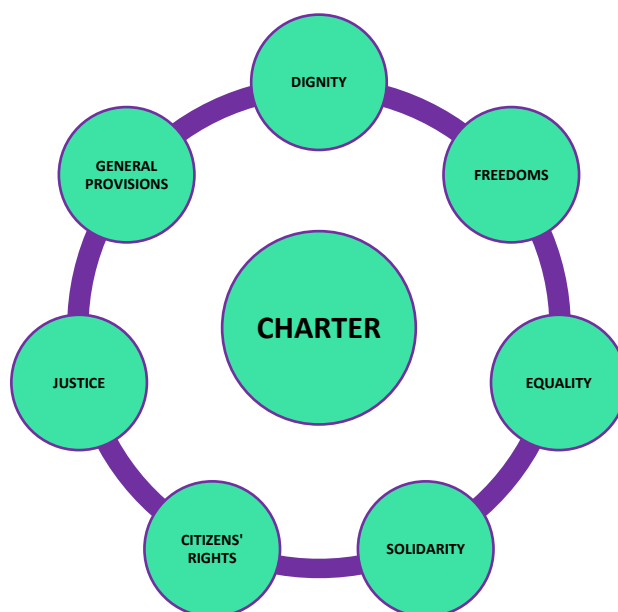


Figure 4: Human Rights protected by the Charter of Fundamental Rights of the EU

The articles that are applicable to our project are Articles 7 and 8.

“Article 7

Respect for private and family life

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

Article 8

Protection of personal data

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.”

Article 7 addresses the right to respect for private and family life. This article emphasizes the importance of individuals' privacy and the need to safeguard their personal information. The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. To take account of developments in technology the word "correspondence" has been replaced by "communications". Article 8 focuses on the principle of non-discrimination. It states that everyone has the right to equal treatment, without discrimination based on various grounds such as sex, race, religion, disability, age, or sexual orientation. Overall, it promotes equality and aims to eliminate any unjust discrimination within the EU while it sets out the conditions under which the personal data are processed and the control of compliance under an independent authority.

Another relevant provision is Article 52 which establishes the principle of proportionality. According to the [Explanations to the Charter](#), the purpose of Article 52 of the Charter is to set the scope of the rights and principles of the Charter, and to lay down rules for their interpretation. It is noteworthy that this provision is not only related to the rights to privacy or data protection but as a general provision related to all fundamental rights enshrined in the Charter of Fundamental Rights of the EU.

2.3.3. The Treaty of the European Union and the Treaty on the Functioning of the European Union

The [TEU](#) was signed in 1992 with main purpose to establish and solidify the European Union (EU) as a political and economic union. The TEU created a framework for cooperation among member states in various areas, such as trade, justice, and foreign policy.

The [TFEU](#), previously known as the Treaty of Rome, was signed in 1957. This treaty aimed to establish a common market within the EU, promoting the free movement of goods, services, capital, and people across member states. The TFEU also outlined the functioning and powers of the EU institutions, such as the European Commission, European Parliament, and European Council.

One important aspect to note is that both treaties are legally binding documents that outline the rights, duties, and objectives of the EU. They lay the foundation for the EU's decision-making processes, institutional structure, and policies.

Both treaties have undergone several amendments and revisions over the years to adapt to evolving challenges and priorities. For example, the Treaty of Lisbon in 2007 introduced changes to improve the efficiency and transparency of the EU's decision-making processes.

Article 16 of the TFEU is of our main interest. It reinforces that data protection is to be considered a fundamental right and lays down the legal basis for all data protection legislation. Moreover, Art. 16 TFEU also restates that the compliance with data processing rules shall be subject to control of an independent authority. The rules adopted on the basis of this Article are without prejudice to the specific rules laid down in Article 39 of the TEU.

2.4. Secondary European Union Legislation

2.4.1. Overview

Secondary EU legislation is a collective term used to describe the laws and regulations enacted by the EU institutions in order to provide further details and implement the goals and provisions outlined in the primary legislation, such as treaties and regulations.

Secondary EU legislation is essential for the effective functioning of the EU as it helps to harmonize laws and regulations across member states, ensuring consistency and coherence in the implementation of EU policies. It provides more specific guidelines and details on how the overarching principles and objectives of the primary legislation should be put into practice.

2.4.2. The General Data Protection Regulation

2.4.2.1. Background and scope of the General Data Protection Regulation

The EU has enacted legislation that addresses specific ethical issues, such as the protection of personal data and privacy. The General Data Protection Regulation (GDPR) is a notable example of such legislation. It harmonizes data protection laws across EU member states, ensuring that individuals have control over their personal information and promoting transparency and accountability from organizations handling personal data. The GDPR is designed to uphold ethical principles such as data minimization, purpose limitation, and the requirement for informed consent.

The [GDPR](#) while drafted and passed by the EU, all organizations around the world that target or collect data related to people in the EU are obliged to comply. The GDPR entered into force in 2016 after passing European Parliament, and as of May 25, 2018, all organizations were required to be compliant. Severe fines against anyone that doesn't respect its privacy and security standards are brought upon.

The Regulation provides a solid legal basis personal data and their processing, protection by design and default, breach and pseudonymization.

2.4.2.2. Key Definitions

Personal data	Data processing	Data subject	Data controller	Data processor
Personal data is any information that relates to an individual who can be directly or indirectly identified, like names and email addresses. Other examples are location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions. Pseudonymous data can also fall under the definition if it's relatively easy to ID someone from it.	Any action that is performed on data, whether it is automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, erasing, etc Article 4(2)	The person whose data is processed.	The person who decides why and how personal data will be processed. Article 4, paragraph 7	A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. Article 4, paragraph 8

Article 4(1) GDPR.				
--------------------	--	--	--	--

Exceptions

The GDPR does not apply to activities outside the scope of EU law.

2.4.2.3. Key Regulatory Points of the General Data Protection Regulation

Data Protection Principles

The GPPR Regulation has been designed to be applicable independently by the technology used for the processing. Processing data has to comply with the seven protection and accountability principles outlined in Article 5 (Figure 5).

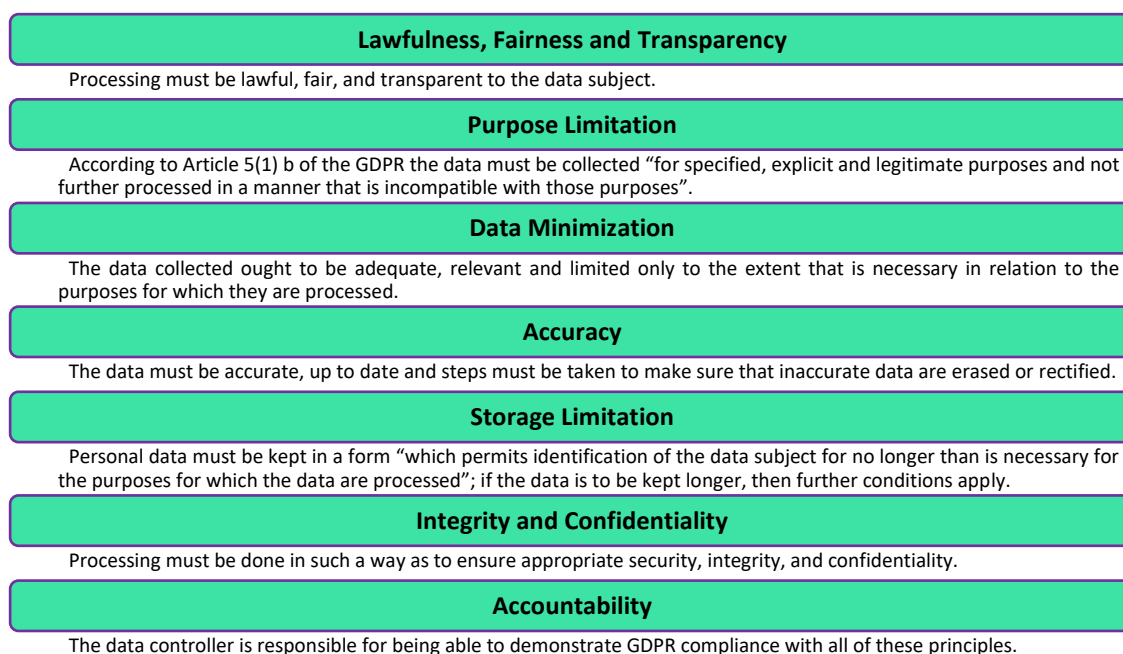


Figure 5: The seven protection and accountability principles

Data Security

Article 32 of the regulation refers to the security of processing. It states that the controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller. They will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- A. the pseudonymisation and encryption of personal data;

- B. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- C. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- D. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Rights of the Data Subject

According to the GDPR, personal data means any information relating to an identified or identifiable natural person: “data subject”. The rights of the data subject are regulated by the Articles 15-22 (Figure 6).

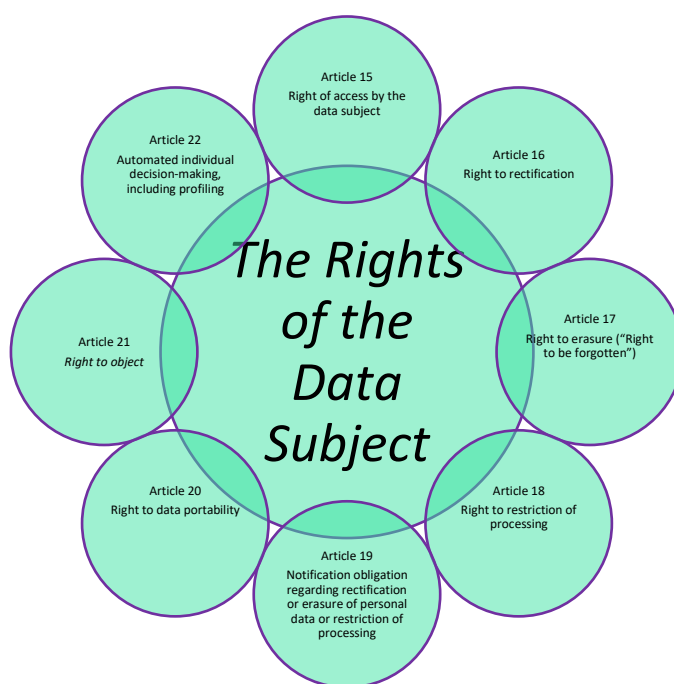


Figure 6: The Rights of the Data Subject according to the General Data Protection Regulation (GDPR)

Consent

Article 6 of the regulation defines the data subject’s consent. Lawfulness in data processing means that personal data can only be handled if it's allowed by a specific legal reason. The GDPR gives six legal bases for this; these bases make it legally okay to handle personal data

- ✓ Consent must be “freely given, specific, informed and unambiguous.”
- ✓ Requests for consent must be “clearly distinguishable from the other matters” and presented in “clear and plain language.”

- ✓ Data subjects can withdraw previously given consent whenever they want, and their decision must be honoured. The legal basis of the processing to one of the other justifications can't simply change.
- ✓ Children under 13 can only give consent with permission from their parent.
- ✓ Documentary evidence of consent must be kept.

2.4.3. ePrivacy Directive

The ePrivacy Directive imposes general obligations regarding the processing of personal data as part of the provision of electronic communications services that are publicly accessible through public networks. Moreover, the material scope of the ePrivacy Directive is significantly broader than just electronic communications service providers, as it includes cookies as well.

Communication is defined as “any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service” (Article 2(d) of the ePrivacy Directive).

Additionally, Article 5(3) and Article 13 of the ePrivacy Directive apply to providers of electronic communication services as well as website operators (e.g., for cookies) or other businesses (e.g., for direct marketing). Also, the use of cookies to create user profiles for advertising or market research purposes requires the users' explicit consent.

The ePrivacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector. It also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications, as enshrined in Article 7 of the Charter of Fundamental Rights of the EU ("Charter").

2.4.4. The ePrivacy Regulation

On the 10th of January 2017, the European Commission released its proposal for a new [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 \(Regulation on Privacy and Electronic Communications\)](#) replacing the 2002 ePrivacy Directive in the electronic communication sector.

This proposal is *lex specialis* to the GDPR and will particularise and complement it as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The alignment with the GDPR resulted in the repeal of some provisions, such as the security obligations of Article 4 of the ePrivacy Directive.

2.4.5 Ensuring compliance with the General Data Protection Regulation principles within the TRUST-FOOD project

The controller is the one who determines the purpose of the processing. This purpose is important for various requirements of the GDPR, including for compliance with its principles. Therefore, it should be clear from the

outset why the personal data will be processed. When and if personal data are used in the context of the project said data must be identified, exposed and discussed with all the Work Package and Task leaders of the TRUST-FOOD project.

3. TRUST – FOOD – Ethics

3.1. General Information

The ethics framework in European projects is designed to protect research participants, promote responsible conduct of research, and uphold the highest ethical standards. It ensures that European-funded projects adhere to ethical principles and contribute to the advancement of knowledge and societal well-being in an ethical and responsible manner.

3.1.1. Grant Agreement – Ethics – General Requirements

As per the project's Grant Agreement and the rules depicted for carrying out the action, Article 14 is dedicated to Ethics and Values in the TRUST – FOOD project.

ARTICLE 14 — ETHICS AND VALUES

14.1 Ethics

The action must be carried out in line with the highest ethical standards and the applicable EU, international and national law on ethical principles.

Specific ethics rules (if any) are set out in Annex 5.

14.2 Values

The beneficiaries must commit to and ensure the respect of basic EU values (such as respect for human dignity, freedom, democracy, equality, the rule of law and human rights, including the rights of minorities).

Specific rules on values (if any) are set out in Annex 5.

14.3 Consequences of non-compliance

If a beneficiary breach any of its obligations under this Article, the grant may be reduced (see Article 28). Such breaches may also lead to other measures described in Chapter 5.

3.1.2. Annex 5 of the TRUST – FOOD Grant Agreement

3.1.2.1. CONFIDENTIALITY AND SECURITY (— ARTICLE 13)

Sensitive information with security recommendation

Sensitive information with a security recommendation must comply with the additional requirements imposed by the granting authority.

Before starting the action tasks concerned, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task. The documents must be kept on file and be

submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary.

For requirements restricting disclosure or dissemination, the information must be handled in accordance with the recommendation and may be disclosed or disseminated only after written approval from the granting authority.

EU classified information

If EU classified information is used or generated by the action, it must be treated in accordance with the security classification guide (SCG) and security aspect letter (SAL) set out in Annex 1 and Decision 2015/4441 and its implementing rules — until it is declassified.

Deliverables which contain EU classified information must be submitted according to special procedures agreed with the granting authority.

Action tasks involving EU classified information may be subcontracted only with prior explicit written approval from the granting authority and only to entities established in an EU Member State or in a non-EU country with a security of information agreement with the EU (or an administrative arrangement with the Commission).

EU classified information may not be disclosed to any third party (including participants involved in the action implementation) without prior explicit written approval from the granting authority.

3.1.2.2. ETHICS (— ARTICLE 14)

Ethics

Actions involving activities raising ethics issues must be carried out in compliance with:

- ethical principles

and

- applicable EU, international and national law, including the EU Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms and its Supplementary Protocols.

The beneficiaries must pay particular attention to the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to the physical and mental integrity of persons, the right to non-discrimination, the need to ensure protection of the environment and high levels of human health protection.

Before the beginning of an action task raising an ethical issue, the beneficiaries must have obtained all approvals or other mandatory documents needed for implementing the task, notably from any (national or local) ethics committee or other bodies such as data protection authorities.

The documents must be kept on file and be submitted upon request by the coordinator to the granting authority. If they are not in English, they must be submitted together with an English summary, which shows

that the documents cover the action tasks in question and includes the conclusions of the committee or authority concerned (if any).

3.1.2.3. INTELLECTUAL PROPERTY RIGHTS (IPR) — BACKGROUND AND RESULTS — ACCESS RIGHTS AND RIGHTS OF USE (— ARTICLE 16)

Definitions

Access rights — Rights to use results or background.

Dissemination — The public disclosure of the results by appropriate means, other than resulting from protecting or exploiting the results, including by scientific or professional publications in any medium.

Exploit(ation) — The use of results in further innovation and deployment activities other than those covered by the action concerned, including among other things, commercial exploitation such as developing, creating, manufacturing and marketing a product or process, creating and providing a service, or in standardisation activities.

Fair and reasonable conditions — Appropriate conditions, including possible financial terms or royalty-free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged.

List of background — Background free from restrictions

The beneficiaries must, where industrial and intellectual property rights (including rights of third parties) exist prior to the Agreement, establish a list of these pre-existing industrial and intellectual property rights, specifying the rights owners.

The coordinator must — before starting the action — submit this list to the granting authority.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, background that is subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions and that impact the results (i.e. would make the results subject to control or restrictions) must not be used and must be explicitly excluded in the list of background — unless otherwise agreed with the granting authority.

Results free from restrictions

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries must ensure that the results of the action are not subject to control or other restrictions by a country (or entity from a country) which is not one of the eligible countries or target countries set out in the call conditions — unless otherwise agreed with the granting authority.

Ownership of results

Results are owned by the beneficiaries that generate them (unless the consortium agreement specifies another ownership regime).

Protection of results

The beneficiaries must adequately protect their results — for an appropriate period and with appropriate territorial coverage — if protection is possible and justified, taking into account all relevant considerations, including the prospects for commercial exploitation, legitimate interests of the other beneficiaries and any other legitimate interests.

Exploitation of results

Beneficiaries must — up to four years after the end of the action (see Data Sheet, Point 1) — use their best efforts to exploit their results directly or to have them exploited indirectly by another entity, in particular through transfer or licensing.

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons (and unless otherwise agreed with the granting authority), the beneficiaries must produce a significant number of products, services or processes that incorporate results of the action or that are produced through the use of results of the action in the eligible countries or target countries set out in the call conditions.

Where the call conditions impose moreover a first exploitation obligation, the first exploitation must also take place in the eligible countries or target countries set out in the call conditions.

The beneficiaries must ensure that these obligations also apply to their affiliated entities, associated partners, subcontractors and recipients of financial support to third parties.

Transfers and licensing of results

Where the call conditions restrict participation or control due to security or EU strategic autonomy reasons, the beneficiaries may not transfer ownership of their results or grant licences to third parties which are established in countries which are not eligible countries or target countries set out in the call conditions (or are controlled by such countries or entities from such countries) — unless they have requested and received prior approval by the granting authority.

The request must:

- identify the specific results concerned
- describe in detail the new owner and the planned or potential exploitation of the results and
- include a reasoned assessment of the likely impact of the transfer or license on the security interests or EU strategic autonomy.

The granting authority may request additional information.

The beneficiaries must ensure that their obligations under the Agreement are passed on to the new owner and that this new owner has the obligation to pass them on in any subsequent transfer.

Access rights — Additional rights of use

Rights of use of the granting authority on results for information, communication, publicity and dissemination purposes

The granting authority also has the right to exploit non-sensitive results of the action for information, communication, dissemination and publicity purposes, using any of the following modes:

- use for its own purposes (in particular, making them available to persons working for the granting authority or any other EU service (including institutions, bodies, offices, agencies, etc.) or EU Member State institution or body; copying or reproducing them in whole or in part, in unlimited numbers; and communication through press information services)
- distribution to the public in hard copies, in electronic or digital format, on the internet including social networks, as a downloadable or non-downloadable file
- editing or redrafting (including shortening, summarising, changing, correcting, cutting, inserting elements (e.g., meta-data, legends or other graphic, visual, audio or text elements) extracting parts (e.g., audio or video files), dividing into parts or use in a compilation
- translation (including inserting subtitles/dubbing) in all official languages of EU
- storage in paper, electronic or other form
- archiving in line with applicable document-management rules
- the right to authorise third parties to act on its behalf or sub-license to third parties, including if there is licensed background, any of the rights or modes of exploitation set out in this provision
- processing, analysing, aggregating the results, and producing derivative works disseminating the results in widely accessible databases or indexes (such as through 'open access' or 'open data' portals or similar repositories, whether free of charge or not).

The beneficiaries must ensure these rights of use for the whole duration they are protected by industrial or intellectual property rights.

If results are subject to moral rights or third-party rights (including intellectual property rights or rights of natural persons on their image and voice), the beneficiaries must ensure that they comply with their obligations under this Agreement (in particular, by obtaining the necessary licences and authorisations from the rights holders concerned).

Access rights for the granting authority and EU institutions, bodies, offices, or agencies to results for policy purposes

The beneficiaries must grant access to their results — on a royalty-free basis — to the granting authority, other EU institutions, bodies, offices or agencies, for developing, implementing and monitoring EU policies or programmes.

Such access rights are limited to non-commercial and non-competitive use.

Access rights for the granting authority to results in case of a public emergency

If requested by the granting authority in case of a public emergency, the beneficiaries must grant non-exclusive, world-wide licences to third parties — under fair and reasonable conditions — to use the results to address the public emergency.

Access rights for third parties to ensure continuity and interoperability


Where the call conditions impose continuity or interoperability obligations, the beneficiaries must make the results produced in the framework of the action available to the public (freely accessible on the Internet under open-source licences).

3.1.3. Grant Agreement – Ethics – Task 1.3 – Ethics Management

Special consideration has been given to the ethics aspect in the TRUST – FOOD project. According to Task 1.3. – Ethics Management:

In order to ensure the implementation of all measures to face the ethical challenges of TRUST-FOOD i.e., the adherence to ethics, we will proceed immediately

- at the inaugural meeting
- to the election of a "TRUST-FOOD Ethics Committee", which will be responsive to the TRUST-FOOD management. This committee will consist of an odd number of TRUST-FOOD members representing the different scientific specialties of TRUST-FOOD and including - and chaired by - an independent authoritative ethics expert not involved in the project, but sufficiently knowledgeable of the scientific issues involved.



TRUST FOOD

Advanced Digital Skills on Blockchain for Trusted Food Supply Chains

Chairperson: Galatia Kapellakou, University of Patras

TRUST-FOOD Ethics Committee	
REZOS	Dimitrios Tsolis (dimitrios@rezosbrands.com)
SAH	Antigolena Folina (antigolena@smartagrohub.gr)
UNIC	Marianna Charalambous (charalambous.mari@unic.ac.cy)
WUR	Pien Schouten
UNI LUX	Dimitris Botsis
UBITECH	Eleni Tsironi
KAU	Aleksandra Pravdyva
482 SOLUTIONS	Leonid Khatskevych
AFC	Ivic Kresimir (ivic@agrifoodcroatia.com)
GREEN POINT	Aleksandra Kocet
AUA	Kostas Demestichas
INSME	Giovanni Zazzerini (zazzerini@insme.org)
ATC	Felix Arion (felix.arion@agrocluster.ro)
LITMEA	Giedrius Bagusinskas

Figure 7: The Ethics Committee's Chairperson and members in the TRUST – FOOD project

The ethics committee will:

- ✓ prepare a "TRUST-FOOD Ethics blueprint", which all TRUST-FOOD team members will agree to abide to
- ✓ examine the compliance of EU and local ethics regulations and their uniformity in each country
- ✓ meet at least once a year to discuss any issues that may arise related to ethics.

The ethics committee will also meet either in person or via teleconferencing whenever events demand its intervention and/or advice.

- ✓ preapprove the design and validate all data handling approaches according to the Ethics blueprint.

All aspects will pass ethical committee scrutiny at the level of the consortium and at the national level (as required by local regulations applicable to each member of the consortium). The pre-approval will precede the application to the local ethics committees.

- ✓ provide guidance to each institution if this is deemed necessary.
- ✓ consider the future ethical issues, which the development of TRUST-FOOD may possibly provoke and examine ways to face these future challenges.

REZOS will be the ethics manager of the project, supported by all involved partners. The project includes implementation of surveys and questionnaires. For this, all GDPR rules (General Da. Off J Eur Union 2016;L119:1–88) will apply. The contribution to the surveys/questionnaires will be voluntary and anonymous. Intellectual Property Rights (IPR) of the educational package developed will be protected according to Horizon 2020 rules (<https://op.europa.eu/en/publication-detail/-/publication/e20da012-ec16-11e9-9c4e-01aa75ed71a1/language-en/format-PDF/source-164620712>).

The related to Task 1.3. deliverable is D1.2 – Ethics Dimension in Research Content.

Deliverable D1.2 – Ethics dimension in research content

Deliverable Number	D1.2	Lead Beneficiary	1. REZOS
Deliverable Name	Ethics dimension in research content		
Type	OTHER	Dissemination Level	PU - Public
Due Date (month)	12	Work Package No	WP1
Description			
The Ethics deliverable. Pdf format, English.			

Figure 8: The Ethics Deliverable in the TRUST – FOOD project

3.1.4. Consortium Agreement – Ethics

3.1.4.1. Article 4, Section 4.4. Specific responsibilities regarding data protection

Where necessary, the Parties shall cooperate in order to enable one another to fulfil legal obligations arising under applicable data protection laws (the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter referred to as “GDPR”) and relevant national data protection law applicable to said Party) within the scope of the performance and administration of the Project and of this Consortium Agreement.

In particular, the Parties shall, where necessary, conclude a separate data processing, data sharing and/or joint controller agreement before any data processing or data sharing takes place.

The Parties shall not in the framework of the Project

(i) disclose to each other Personal Data; or

(ii) Process Personal Data if and to the extent two or more Parties are joint controllers (as defined in Article 26 of GDPR)

without separate arrangement accepted by the Parties in writing for such purpose, except for the necessary Personal Data of persons participating in the Project or conclusion of this Consortium Agreement.

3.1.4.2. TRUST – FOOD Project Ethics Committee

The Project Ethics Committee, which will be responsive to the Project Technical Committee (PTC). This committee will consist of TRUST-FOOD members representing the different scientific specialties of TRUST-FOOD and including - and chaired by - an independent authoritative ethics expert not involved in the project, but sufficiently knowledgeable of the scientific issues involved. Since there is no budget foreseen for the remuneration of independent authoritative ethics expert dedicated to the project, each partner has to take this under consideration in order to propose the ethic experts who are willing to participate as independent authoritative ethics expert without any remuneration. In case of mandatory physical presence of the expert to a project meeting for example by the Project Officer, travel expenses have to be agreed between partners proportionally to each partner’s budget, or by any other means that will be decided between all partners at the PCC.

The Coordinator will ensure that a non-disclosure agreement is executed between the Coordinator and the independent ethics expert(s).

3.2. Transfer and Use of Personal Data

Personal data will NOT be transferred to EU nor to non-EU Countries and will not be accessed/accessible from EU and non-EU Countries (Ukraine). The data used will only include data extracts and user generated content from the digital training platform and the mobile application. The data will be extracted as statistical data sets and will be transferred as raw data to the Trust-Food infrastructure. In every case and when necessary, the data will be anonymized and homogenized so as to be further elaborated and used as

statistical data and for monitoring the project's KPIs. The rights of the research participants are fully safeguarded based on national and EU legislation as applied to each partner's country. In addition, TRUST - FOOD complies with the General Data Protection Regulation, GDPR, for collection, storing and managing research data (Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC). GDPR is applied by all the partners of the project based on national and EU legislation which is legally binding all the processes and information produced by the partnership (even if personal data isn't being transferred and / or accessed by EU or Non-EU countries).

The project, even if isn't using or re-using personal data, utilizes all the necessary technical measures, fully aligned with the EU Guidelines, so as to prevent unauthorized access to data. The data sets used are fully anonymized. Data anonymization methods used in the project adhere to strict data privacy regulations which require the security of personally identifiable information (PII), such as health reports, contact information, and financial details to be permanently erased. The technique used is data masking with which data are substituted by modified values. Data anonymization is done by creating a mirror image of a database and implementing alteration strategies, such as character shuffling, encryption, term, or character substitution. The data minimization principle will be fully applied.

In addition, Trust-Food complies with the General Data Protection Regulation, GDPR, for collection, storing and managing research data with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC). The project's researchers will not re-use personal data, such as names, identities and addresses. No sensitive data, in addition, such as that on health, sexual lifestyle or the religious conviction of people will be collected. Personal data isn't necessary to achieve the research task and therefore personal data will not be collected. The project will make sure that data collected in the project is protected by adequate organizational and technical arrangements. These arrangements will be of such kind that it will ensure an appropriate security level in relation to the risks of collecting and storing the data. No personal data will be transferred to EU nor to non-EU countries.

3.3. Non-EU Countries

Benefits-sharing especially for Ukraine as a non-EU low- and middle-income country means ensuring fair sharing of new values produced from the research activities in Ukraine. Stakeholders in Ukraine, including researchers and trainees should see those benefits rising from Trust-Food project is shared in a fair way between all parties. Trust-Food promotes openness and co-ownership of the research and its outcomes. Co-creation is a key element of the project, as each work package requires inputs from partners both in and outside EU, especially for developing the services and applications. Ukraine will also have full access to the research results produced in other country case studies, which can be a valuable source of lesson learning for all partner institutions. Research results will be promoted to Ukraine through the respective partner organizations. Researchers from Ukraine are also participating in knowledge creation through participation in developing and/or implementing the infrastructure and the services.

4. References

Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), 2016. Available at: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189>

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, 2000. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

CONSOLIDATED VERSION OF THE TREATY ON EUROPEAN UNION, 2012. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF

CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION, 2012. Available at: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF>

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. Available at: <https://rm.coe.int/1680078b37>

Convention for the protection of individuals with regard to the processing of personal data, 2018. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf

Cybercrime Convention Committee, <https://www.coe.int/en/web/cybercrime/tcy>

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 sector (Directive on privacy and electronic communications), 2002. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058>

European Convention on Human Rights, 1950. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG

EXPLANATIONS (*) RELATING TO THE CHARTER OF FUNDAMENTAL RIGHTS, 2007. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007X1214(01))

General Data Protection Regulation (GDPR), 2018. Available at: <https://gdpr.eu/tag/gdpr/>

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), 2017. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010>

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 2018. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (Text with EEA relevance), 2021. Available at: <https://eur-lex.europa.eu/eli/reg/2021/695/oj>

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), 2022. Available at: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyenum=224>