D1.2. Initial Version of Legal, Ethical and Data Management Report

Submission date: 28 June 2024
Due date: M06 (June 2024)

DOCUMENT SUMMARY INFORMATION

Grant Agreement No	101136583		
Full Title	AN INTEGRATED APPROACH TO ENHANCE FOOD SYSTEMS RESILIENCE, ADVOCATING FOR FOOD SECURITY AND UNINTERRUPTED FOOD SUPPLY		
Start Date	01/01/2024	Duration	42 months
Deliverable	D1.2: Initial Version of Legal, Ethical and Data Management Report		
Work Package	WP1 – Project Coordination		
Type	R	Dissemination Level	PU
Lead Beneficiary	Laurea University of Applied Sciences (LAU)		
Authors	Tuomas Tammilehto (LAU)		
Co-authors			
Reviewers	Sofia Kordouli (ED), Georgios Kolionis (EXUS)		
Abstract	This document summarises the ethical and data protection considerations for the project's practices and outputs		

This project has received funding from the European Union's Horizon Europe research and innovation program under Grant Agreement No. 101136583.
The material presented and views expressed here are the responsibility of the author(s) only.
The European Commission takes no responsibility for any use made of the information set out.

DOCUMENT HISTORY

Version	Date	Changes	Contributor(s)
V0.1	15/2/2024	Toc	LAU
V0.2	23/6/2024	Sent for internal review	LAU
V0.3	27/6/2024	Review	Georgios Kolionis (EXUS) and Sofia Kordouli (ED)
V0.4	28/6/2024	Review comments acknowledged	Tuomas Tammilehto (LAU)
V1.0	29/6/2024	Final version	ED

About SecureFood

The European Union's (EU) Farm to Fork strategy, the Biodiversity strategy and the European Green Deal, lay down important actions that set a long-term vision concerning the change of the way we produce, distribute, and consume food.

In response to these ambitious aims, **SecureFood** adopts an integrated systems-thinking approach that acknowledges and embraces the complexity of the food supply chain, including all the actors, elements, processes, activities, infrastructure and essential services of importance in the production, distribution and consumption of food in order to maximize the food supply chain resilience.

The goal of **SecureFood** is to create an ecosystem of scientific knowledge, collaborative processes, and digital tools that will provide evidence-based indications of the risks and vulnerabilities of the different food value categories in different geographies in order to safeguard food security and to ensure that a secure and resilient food supply chain is assured.

The two crucial **pillars** of the program are the **Food Systems Resilience Management Framework** with connected resilience and sustainability orientations, as well as a **Resilience Governance Framework** that draws upon all of the collaborative principles and guidelines of the successful cooperation between the food supply chain stakeholders, which will be created, tested, and demonstrated in real life case studies. These two frameworks will function as applicability and sustainability mechanisms for organizing and adopting the project's results by applying the developed scientific knowledge, and by enhancing the food system resilience at different levels.

The **ambition** of the program consists of four critical dimensions, which are: 1) the evolution of scientific knowledge and development of the exploratory approach, combining research approach methods that facilitate the risk identification process; 2) the successful safeguarding of the food supply by framing the system resilience and broadening its lens, as well as by assessing and measuring it through a holistic approach which goes beyond national borders and strategies; 3) the acceleration of the transformation of the food systems network, which can be achieved by applying a systematic agency driven collaborative governance approach; 4) and finally, the application of innovative scientific knowledge with the use of advanced digital tools, which will contribute to the successful collection and processing of data sets from several platforms to reshape and redesign the food system trajectory.

The methodology employed is based on three foundational and interconnected elements: the scientific knowledge (existing and developing), the collaborative principles which are dynamically integrated into the methodology, as well the development of digital solutions which will cover all parts of the project (forecasting, statistical analysis etc.)

PROJECT PARTNERS

Partner	Country	Short name
EUROPEAN DYNAMICS LUXEMBOURG SA	LU	**ED**
EUROPEAN DYNAMICS ADVANCED INFORMATION TECHNOLOGY AND TELECOMMUNICATION SYSTEMS SA	*EL*	***EDAT***
ERGASTIRIA GALANAKIS E E	EL	**GL**
FUNDACION ZARAGOZA LOGISTICS CENTER	ES	**ZLC**
EMPRACTIS E.E. SYMVOULOI MICHANIKOI	EL	**EMP**
DNV BUSINESS ASSURANCE ITALY SRL	IT	**DNV**
IRIS TECHNOLOGY SOLUTIONS, SOCIEDAD LIMITADA	ES	**IRIS**
LEIBNIZ-INSTITUT FUER AGRARENTWICKLUNG IN TRANSFORMATIONSOEKONOMIEN (IAMO)	DE	**IAMO**
EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON	EL	**ICCS**
LAUREA-AMMATTIKORKEAKOULU OY	FI	**LAU**
EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS	EL	**EXUS**
INNOV-ACTS LIMITED	CY	**INNOV**
CARR COMMUNICATIONS LIMITED	IE	**CARR**
COSMOSHIP MARITIME LIMITED	CY	**COSMO**
NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE	UA	**NULES**
MINISTRY OF AGRARIAN POLICY AND FOOD OF UKRAINE	UA	**MINAG**
ALL-UKRAINIAN PUBLIC ORGANISATION UKRAINIAN AGRARIAN CONFEDERATION	UA	**UAC**
ASSOCIATION UKRAINIAN AGRIBUSINESSCLUB	UA	**UCAB**
ELLINIKOS GEORGIKOS ORGANISMOS - DIMITRA	EL	**ELGO**
LUONNONVARAKESKUS	FI	**LUKE**
ENOSI KATANALOTON POIOTITA TIS ZOIS	EL	**EKP**
ROUSSAS ANONYMI ETAIREIA	EL	**ROUS**
SPREAD EUROPEAN SAFETY AND SUSTAINABILITY GEIE	IT	**SPES**
FEDERAZIONE ITALIANA DELL INDUSTRIAALIMENTARE ASSOCIAZIONE	*IT*	***FEDAL***
ASSOCIATION NATIONALE DES INDUSTRIES ALIMENTAIRES	*FR*	***ANIA***
FEDERACAO DAS INDUSTRIAS PORTUGUESAS AGRO-ALIMENTARES	*PT*	***FIPA***
FEDERACION ESPANOLA DE INDUSTRIAS DE LA ALIMENTACION Y BEBIDAS	*ES*	***FIAB***
SYNDESMOS ELLINIKON VIOMICHANION TROFIMON SOMATEIO	*EL*	***SEVT***
TUERKIYE SUET ET GIDA SANAYICILERI VE UERETICILERI BIRLIGI DERNEGI	*TR*	***SETBIR***
GOSPODARSKA ZBORNICA SLOVENIJE	*SI*	***CCIS***
LEBENSMITTELVERSUCHSANSTALT	*AT*	***LVA***
POTRAVINARSKA KOMORA CESKE REPUBLIKY	*CZ*	***FFDI***
BIGH SA	BE	**BIGH**
MC SHARED SERVICES SA	PT	**MC**
MODELO CONTINENTE HIPERMERCADOS S.A.	*PT*	***MCH***
ELAFINA ANONYMI ETAIREIA	EL	**ELAF**

Table of Contents

LIST OF FIGURES

LIST OF TABLES

List of Abbreviations and Acronyms

Acronym	Meaning
CA	Consortium Agreement
DoA	Description of Action
DPO	Data Protection Officer
EC	European Commission
EM	Ethics Manager
GA	Grant Agreement
GDPR	General Data Protection Regulation
REB	Regulation and Ethics Board
WP	Work Package

Executive Summary

Titled as the Initial Version of Legal, Ethical and Data Management Report from SecureFood's Work Package 1, emphasising the Ethics Management of this SecureFood project, this document summarises the main legal, ethical and data management points that the project needs to pay attention to in its action. Starting from the Ethics Standards, moving into consent and personal data all the way to misuse and presenting the "methodology" of the ethics work.

It must be highlighted that all project collaborators are collectively responsible for closely adhering to the various ethical aspects in order that our project and its execution is done ethically correctly. However, as said many times, in ethics the questions are often far more important than the answers, since only first by asking the question one can begin the quest for reaching answers. Therefore, this document is also an invitation to start questioning together about ethics and legal aspects. The project has dedicated an Ethical Manager to be the guide in this mission. Please do not hesitate to speak out.

1 Introduction

1.1 Purpose of the Document

SecureFood, an €8 million Horizon Europe project funded under Grant Agreement No. 101136583, was conceived as a response to the evolving challenges in food systems that recognises the intricate web of factors that influences their functionality and stability.

SecureFood project's Description of Action (DoA) Part A describes deliverable D1.2 "Initial version of legal, Ethical and Data Management Report of the Works Package 1 "Project Coordination" as a document in which different ethical and data protection considerations for the project's practices and outputs needs to be covered.

This document starts with the big picture, i.e., European fundamental values and different research guidelines and codes of conduct that SecureFood is going to follow.

Then this deliverable moves into more tangible issues, presenting human participation to the SecureFood activities, and here the main focus is the so-called informed consent of the participants. Therefore, in this deliverable we clarify and explain the procedures to be followed by the SecureFood Consortium regarding humans' involvement in research and provide the respective templates of Information sheet and Consent form, and Information on collecting personal data, as well as the relevant consent form.

The following topic is also heavily related with the human participants and is about the personal data that may or may not be collected during the course of the project. For example, unauthorized access to personal data or the equipment used for processing must be prevented. Thus, all the partners need to have adequate security measures, for example, strong password policy, two Factor Authentication (2FA) and multifactor authentication, physical security practices, monitoring user activity, endpoint security etc.

In addition, if and when needed, proper anonymisation and/or pseudonymisation techniques will be implemented, as well as those partners who will process previous collected data will need to disclose their lawful basis for it, as well have in place the appropriate technical and organisational measures to safeguard the rights of the data subjects.

Furthermore, if there are any research activities that involve tracking of behaviour, the SecureFood partners need to provide explanations how the data subjects will be informed as well as described the possible consequences of the tracking and how the fundamental rights of the tracked individuals will be safeguarded.

Yet again, one thing related to the personal data is the possible data transfers to and from a member state to non-EU member state. In this SecureFood project we have partners from Ukraine, thus we need to confirm that the data transfers according to Section V of GDPR.

Finally, there is the challenge of possible misuse of our research outputs, so there is a section on this too. It is very much related with the first area i.e., with the ethics standards showing that in ethics, everything tends to be intertwined and linked with each other.

Lastly there will be presented the so-called methodology for the ethics work in SecureFood project.

This document has covers somewhat the D9.1 POPD - AI - EPQ - H - NEC - Requirement No. 1, as this deliverable touch many of the issues that will be reported in the D9.1. The main difference is that in this D1.2 Initial Version of Legal, Ethical and Data Management Report the emphasis in on the word initial, as well as on the methodology on collecting the information needed for the D9.1 as well as the justifications and reasonings behind pure technical reporting on how to fulfil requirements toward our funder – the European Commission.

1.2 Structure of the Document

Chapter 1 – Introduction:

This chapter provides an introduction to the topic.

Chapter 2 – Ethics Standards:

This chapter presents the various ethics standards that SecureFood partners have agreed to comply with.

Chapter 3 – Informed Consent for the Participation of Humans in Research Activities:

This chapter describes the so-called informed consent for the participation of humans in research activities as well as informed consent for processing of personal data.

Chapter 4 – Protecting Personal Data:

This chapter presents the different ways with which SecureFood ensures the protections of personal data: DPO, Data Protection Policy, anonymization and pseudonymization techniques, further processing of personal data, tracking behaviour and informing data subjects.

Chapter 4 – Potential Misuse and Counter-measurements:

Here are presented the possible unethical uses of the research findings and some mitigation ways.

Chapter 5 – Ethics "Methodology" and future work

This chapter will present the ways ethics is brought in tangible ways into the project's everyday life together with few words on the future work

1.3 Intended Audience

This document is intended to support SecureFood partners in the effective and efficient ethical management of the project, however, it presents also important aspects on ethics for anyone interested in EC funded projects and the ethical management of them.

1.4 Relationship to other SecureFood deliverables

This document sets the initial steps toward good ethical management of a project. Together with other deliverables touching management and the execution of the project, for example, the *D1.1 Project management and quality assurance handbook*, the *D8.1 Communication and Dissemination Strategy*, and the *D1.3 Data Management Plan (v1)*, they all form a solid backbone for the management of the project as well as assure the correct ways of executing the needed SecureFood activities.

2 Ethical Standards

A very crucial aspect on ethics management is the commitment to EU values, such as respect for human dignity, freedom, democracy, equality, the rule of law and human rights, including the rights of minorities. Furthermore, consortium members have agreed to follow ethical standards, not forgetting applying them too. This needs to do regardless of the country in which the research is conducted.

By signing the SecureFood Grant Agreement (GA),[1] all beneficiaries have agreed to conduct the project in compliance with:

1. Ethical principles, including the highest standards of research integrity.
2. Applicable international, EU, and national laws.

The list of the various codes of conducts and such are:

1. the Helsinki Declaration Administrative forms[2];
2. the European Code of Conduct for Research Integrity[3];
3. the EU Charter on Fundamental Rights[4];
4. the UNESCO Universal Declaration on Bioethics and Human Rights[5];
5. the European Convention for the Protection of Human Rights and Fundamental Freedoms[6]; and
6. the Universal Declaration of Human Rights[7].

Therefore, for example, all beneficiaries have agreed not to:

1. Aim at human cloning for reproductive purposes.
2. Intend to modify the genetic heritage of human beings in a way that could make such changes heritable (except for research related to cancer treatment of the gonads, which may be financed).
3. Intend to create human embryos solely for research or for stem cell procurement, including by means of somatic cell nuclear transfer.

While these activities are highly unlikely given the aim and scope of SecureFood and its research activities, beneficiaries must still respect the fundamental principle of research integrity, as outlined for example in the European Code of Conduct for Research Integrity. This includes adhering to fundamental principles such as:

[1] As per Article 14 and Annex 5 of the Grant Agreement
[2] https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/
[3] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[5] https://www.unesco.org/en/ethics-science-technology/bioethics-and-human-rights
[6] https://www.echr.coe.int/documents/d/echr/convention_ENG
[7] https://www.un.org/en/about-us/universal-declaration-of-human-rights

1. Reliability in ensuring the quality of research, reflected in the design, methodology, analysis, and use of resources.
2. Honesty in developing, undertaking, reviewing, reporting, and communicating research in a transparent, fair, and unbiased manner.
3. Respect for colleagues, research participants, society, ecosystems, cultural heritage, and the environment.
4. Accountability for the research from idea to publication, including management, organization, training, supervision, mentoring, and considering its wider impacts.

As stated earlier, ethical standards and guidelines must be applied consistently, regardless of the country in which the research is conducted, with a particular focus on the location of the research. Due to long-standing cooperation with the Commission, EU member states have harmonized much of their ethical standards for EU research. Some attention thus needs to be put perhaps to the consortium members from non-member states, however, this does not to imply that they are less committed to European values and research integrity.

3 Consent

This chapter will describe the so-called informed consent for the participation of humans in research activities as well as informed consent for processing of personal data.

3.1 Informed Consent for the Participation of Humans in Research Activities

What is informed consent? In the Directive 2001/20/EC[8] Informed Consent is defined in relation to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use:

> *"Informed Consent is the decision, which must be written, dated and signed, to take part in a clinical trial, taken freely after being duly informed of its nature, significance, implications and risks and appropriately documented, by any person capable of giving consent or, where the person is not capable of giving consent, by his or her legal representative; if the person concerned is unable to write, oral consent in the presence of at least one witness may be given in exceptional cases, as provided for in national legislation."*

Although SecureFood is not conducting clinical studies or researching medicinal products, the principles of informed and voluntary consent are still essential for our project. This principle is fundamental to any research activity, emphasizing the importance of written, dated signatures, informing participants, and documenting necessary details.[9]

Ensuring free and voluntary participation through informed consent is crucial for research. Without it, the risk of data distortion would significantly undermine the validity of the research findings. Therefore, research activities must be conducted based on the participants' consent.

To maintain ethical standards, SecureFood, like every Horizon Europe funded project, must respect human dignity, ensure fair distribution of research benefits and burdens, and comply with ethical principles and applicable international, EU, and national laws.[10] Protecting the freedoms, rights, and interests of research participants is of paramount importance.

Therefore, informed consent forms are mandatory. In SecureFood, we provide participants with sufficiently detailed information about the research activities to enable them to make an informed, voluntary, and rational decision to participate.

The Information Sheet includes at minimum:

[8] https://eur-lex.europa.eu/eli/dir/2001/20/oj

[9] When people are working remotely, not face-to-face in same physical space, this has and can be been problematic. Consent is therefore sometimes the action itself: if someone participates willingly on a discussion online, knowing their sayings may be used for research purposes etc., the consent is then asked orally (or in a chat of the online working tool), and the permission has been given orally and confirmed by the participant's continuous participation in the research activities.

[10] The obligation is stated in legislation, but the true compulsion comes from the principles of responsible conduct of research. The principles of voluntary participation and informed consent have been stressed by various scholarly associations practically on every research field long before they epitomised as laws and regulations.

1. Details of the project in general and of the type and purpose of the specific research activity
2. Recruitment criteria, i.e., why they have been chosen to participate.
3. Confirmation of the voluntary character of the research activity.
4. Information on their right to decline or withdraw at any time without any consequences.
5. Location and expected duration of the specific research activity.
6. Potential risk, discomfort, or adverse effects.
7. Prospective research benefits.
8. Information on whom to contact for questions and for the exercise of their rights related to the research.

Participants must be given sufficient time to ask questions about their participation without compromising the research objectives. Therefore, informed consent procedures must be followed whenever SecureFood research activities involve human participation, such as interviews, questionnaires, workshops, brainstorming events, etc. This applies even if most participants are consortium members. However, if all participants are consortium members, then the consent is redundant e.g., for internal brainstorming etc. Otherwise, everyone's voluntary participation must be ensured.

Recruitment criteria may vary based on the nature and purpose of each research activity. Participants may be members of the SecureFood Consortium, members of similar projects, or external stakeholders. In all cases, they will be legally competent adults participating due to personal or work-related interest, profession, knowledge, or expertise. Participants will be informed beforehand about why they were chosen, their role, and the required input.

Before any SecureFood research activity, researchers must inform participants that participation is voluntary, and they have the right to refuse or withdraw at any time without consequences.[11] Participants will receive sufficient information about the research activities in the form of an Information Sheet, distributed in advance and written in easily understandable terms.

A written Consent Form, provided in necessary languages and intelligible terms, must be signed before commencing any activities. Participants should have enough time to read and understand the documents without feeling coerced into giving consent.

Additionally, the names and contact details of the persons responsible for the research must be clearly provided.

3.2 Informed Consent for Processing of Personal Data

At times, it is necessary to collect and process personal data for research or other purposes. While we do not anticipate significant processing of personal data in SecureFood activities, clear guidelines must be established if such cases arise. This includes providing necessary information sheets and obtaining informed consent forms.

[11] There is some ambiguity to this when individuals are participating to research activities as part of their occupation and/or representing their organisations, i.e., whether the involvement is truly voluntary. Therefore, the principle of voluntary participation is stressed to all the partners to avoid such situations, e.g., that the organisations will not force anyone unwilling to participate in SecureFood activities to begin with.

This requirement is grounded in the General Data Protection Regulation (GDPR). According to GDPR, when personal data is processed, researchers or data controllers conducting interviews, questionnaires, or other activities with healthy volunteers, as in SecureFood, must inform participants in advance. This is done through a detailed Information Sheet.

Per Article 13 (1) and (2) of GDPR, when personal data is collected from a data subject, the controller must provide the data subject with the following information at the time the personal data is obtained:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;
2. the contact details of the data protection officer, where applicable;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party
5. the recipients or categories of recipients of the personal data, if any;
6. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to above, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

1. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
2. 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;
3. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
4. the right to lodge a complaint with a supervisory authority;
5. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
6. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

According to Article 7 of the GDPR, when processing is based on consent, the controller must be able to demonstrate that the data subject has consented to the processing of their personal data. If consent is given in a written declaration that includes other matters, the request for consent must be clearly distinguishable, using clear and plain language, and

presented in an intelligible and easily accessible form. Any part of such a declaration that infringes on the GDPR is not binding.

The data subject has the right to withdraw their consent at any time, and this withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. The data subject must be informed of this right before giving consent, and it must be as easy to withdraw consent as it is to give it. The Information Sheet will be in English, a language familiar and understandable to all participants, and translated if necessary. Participants can contact the ethical manager/researcher/data controller for clarifications.

A copy of the Information Sheet will be provided to ensure participants can read it at any time and exercise their rights. Informed consent is crucial for both participation and data processing. SecureFood ensures participants receive adequate information about data processing activities and give their consent freely by filling in and signing an Informed Consent Form.

Consent will generally be in writing, but an oral statement may be used. After ensuring the participant has read and understood the Information Sheet, the researcher/data controller will provide an Informed Consent Form for Data Processing, which the participant will sign. Participants can withdraw their consent at any time without consequences, and personal information on the consent form will be processed in compliance with the GDPR.

The Informed Consent Form will be in English and translated if needed. Participants can contact the responsible person/researcher/data controller for any questions or clarifications.

Given the nature of the data collected in SecureFood, personal data will not be used for future research or purposes other than our current research. Thus, explicit consent for secondary use is not needed. This will be updated during the project course of actions.

3.3 Storage

The templates and information sheets will be stored in SecureFood's online repository (ProofHub), providing all consortium partners with access. Partners can also request these documents from the Ethics Manager to be sent via email.

The responsibility for collecting signed consent forms lies with the organiser of the research activity. These signed informed consent forms will be securely stored by the data controller for the period specified in the SecureFood Grant Agreement (GA), which is five years after the project's completion, to ensure accountability.

The data controller will implement technical, organisational, and security measures to guarantee secure storage.

3.4 Conclusion on consent

Taking the consent to participate in research activities and the consent for processing personal data seriously, we have established procedures and created related templates for the consortium to use.

This deliverable does not replace the work of the Ethical Manager. On the contrary, the Ethical Manager will provide continuous guidance throughout the project, such as advising on how to complete the forms and, if necessary, rephrasing the templates. In ethics, the priority is ensuring that actions are ethical, although formalities must also be properly addressed.

4 Protecting Personal Data

To ensure the ethical integrity of the SecureFood project, it is crucial to respect the fundamental rights enjoyed by individuals in today's European Union. One key right is the protection of natural persons concerning the processing of personal data. For instance, Article 8 (1) of the Charter of Fundamental Rights of the European Union12 and Article 16 (1) TFEU affirm that everyone has the right to the protection of personal data concerning them. Additionally, the European Union has enacted legislation on the protection of natural persons regarding the processing of personal data and the free movement of such data (EU 2016/679 GDPR).

This latter legislation includes the designation of a Data Protection Officer (DPO), where applicable, as a key element to ensure GDPR compliance and safeguard data subjects' rights. The SecureFood consortium, recognising the importance of these measures, acknowledges that protecting personal data throughout its research activities is imperative.

4.1 DPO and Data Protection Policies

4.1.1 DPO

A Data Protection Officer (DPO) is an employee of the organization (Data Controller) or an external expert responsible for ensuring GDPR compliance. The DPO provides expert advice on data protection, educates staff on compliance requirements, addresses questions and inquiries from data subjects, and acts as a point of contact for the data protection supervisory authority.

According to Article 39 of the GDPR, the DPO has at least the following tasks:

1. Inform and advise the controller, the processor, and employees who process data of their obligations under this Regulation and other relevant data protection laws.
2. Monitor compliance with the GDPR, other relevant data protection laws, and the policies of the controller or processor regarding personal data protection, including assigning responsibilities, raising awareness, training staff involved in processing operations, and conducting related audits.
3. Provide advice on data protection impact assessments and monitor their performance as required by Article 35.
4. Cooperate with the supervisory authority.
5. Serve as the contact point for the supervisory authority on issues related to processing, including prior consultation as referred to in Article 36, and consult on any other relevant matters.

In performing these tasks, the DPO must consider the risks associated with processing operations, taking into account the nature, scope, context, and purposes of the processing.

[12] https://www.europarl.europa.eu/charter/pdf/text_en.pdf

For consortium members who have appointed a DPO, this person plays a crucial role in ensuring compliance with applicable data protection rules and serves as the main contact point for data subjects, especially regarding the exercise of their rights.

Per Articles 13(1)(b) and 14(1)(b) of the GDPR, data subjects must be provided with the DPO's contact details. During the SecureFood project, any activities involving the processing of personal data will be conducted only after the DPO's contact details have been made available to the data subjects. If a DPO is not required, for example, if the consortium member is a SME, the relevant Data Protection Policy will be explained, typically via appropriate information sheets.

To this end, the SecureFood beneficiaries will be asked to share the contact details of their DPOs as well the Data Protection Policies.

4.1.2 Data Protection Policy

A detailed data protection policy needs to be prepared by those who are not required to designate a DPO under article 37 par.1 of the GDPR. (See the Annex for detailed model policy). This data protection policy includes, among others, details on the types of personal data processed, the purposes of processing, the respective legal bases, the storage period, and the data subjects' rights. These will be collected from the consortium members tooas well.

4.2 Unauthorised Access to Personal Data

Preventing unauthorised access to personal data is both a fundamental security and ethical issue that SecureFood must address. The security measures implemented to prevent unauthorized access to personal data that the consortium members are taking will be collected and describes in a format of a table (see below Table as an example). This table will be updated when needed. The ways of updating will be described later in this document.

Partner	The security measures to prevent unauthorized access to personal data	The equipment used for processing personal data
LAU	Data security is ensured with continuous, extensive actions in close and constructive cooperation between all the people and groups included in the university community. Proper data security implies continuous monitoring of operations, long-term planning, preparation for various risks and threats, compliance with agreed procedures, instructions, training and communication. In addition to technical equipment, proper data security requires competent end users who are aware of the impact of their actions on their own and others' security. Everyone has personal accounts, Laurea's computer's hard drives are encrypted, strong password policy, Firewalls, Virus protection, Secure Print Release work with ID card etc.	University's laptops and ProofHub (a service environment for electronic work and networking provided by the coordinator). ProofHub enables flexible and secure collaboration across organizational boundaries, collaborative online system in which each user has their own user ID and password for the systems. The data is collected into databases that are protected by firewalls, passwords and other technical measures. The databases and backups of these databases are located in locked facilities and only previously selected individuals have access to this data.

Table 4-1: Example of security measures and equipment

4.3 Anonymization and Pseudonymisation techniques

Also related to the protection of personal data are the techniques of anonymization and pseudonymisation, i.e., techniques that can be used to protect the personal data of any research subject.[13] The consortium partners will be asked whether they use any of them, naturally depending on their need to use any personal data.

4.3.1 Anonymization

According to the Office of the Data Protection Ombudsman of Finland, anonymization involves processing personal data so that individuals can no longer be identified. This can be achieved by reducing data to a general level (aggregated) or converting it into statistics. The

[13] For further details, see GDPR: articles 2, 4(1), 4(5); recitals 14, 15, 26, 27, 29, 30 (EUR-Lex), and also Opinion 4/2007 on the concept of personal data (Online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf), Opinion 05/2014 on Anonymisation Techniques (Online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

prevention of identification must be permanent, ensuring neither the controller nor a third party can revert the data to an identifiable form with the information they possess.

Anonymization must consider all reasonably viable methods for reverting data back to an identifiable form, including the costs, time, and available technologies. The controller must also anticipate that over time, advancements in technology could weaken anonymization.

Anonymized data are no longer classified as personal data and are not subject to data protection regulations. However, determining whether data is truly anonymous requires case-by-case evaluation. Individuals can often be identified by other data points, so simply removing names and direct identifiers may not suffice. Detailed information, such as rare diseases or a combination of data types, can still make individuals indirectly identifiable.

If a controller discloses a data set with any remaining identifiable information, it is still considered personal data, and its processing remains subject to data protection regulations.

4.3.2 Pseudonymization

Pseudonymization, on the other hand, involves processing personal data so it cannot be attributed to a specific person without additional information, which must be kept separate from the personal data. For instance, encoding personal data is a form of pseudonymization. Encoded data cannot be linked to an individual without a code key, but the holder of the code key can still decode the records and identify the data subjects.

Pseudonymized data can still single out individuals and link their data from different records, meaning it is still considered personal data and is subject to data protection regulations. For example, using false names in a database replaces the original data but still allows for the identification and combination of individual records.

4.4 Further processing of previously collected personal data

Yet again one thing related to personal data is the further processing of previously collected personal data. This is not likely in SecureFood project activities, but in case any consortium member encounters this situation in their activities, this needs to be clarified too.

According to the European Commission, the purpose for processing personal data must be clear, and the individuals whose data is being processed must be informed.[14] Merely stating that personal data will be collected and processed is insufficient. This is known as the 'purpose limitation' principle.[15]

The 'purpose limitation' principle significantly restricts the use of previously collected personal data, but it does not completely prohibit it. If data is collected based on *legitimate interest*[16],

[14] EC https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing_en

[15] See, Opinion 03/2013 on purpose limitation. Online at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[16] "The processing of personal data can be in the legitimate interests of the controller, for example, when there is a relevant relationship between the controller and data subject. In practice, this means that the data subject is the customer or subordinate of the controller.

it can be used for another purpose only after verifying that the new purpose is compatible with the original purpose.

To ensure compatibility when processing personal data for a new purpose, the following points must be considered:

1. The link between the original purpose and the new purpose.
2. The context in which the data was collected (e.g., the relationship between the organization and the individual).
3. The type and nature of the data (e.g., whether it is sensitive).
4. The possible consequences of the intended further processing (e.g., how it will impact the individual).
5. The existence of appropriate safeguards (e.g., encryption or pseudonymization).

If an organization wants to use the data for statistics or scientific research, it is not necessary to conduct the compatibility test. Additionally, if data was collected based on consent or a legal requirement, no further processing beyond what is covered by the original consent or legal provisions is allowed. Further processing would require obtaining new consent or establishing a new legal basis.

Again, the partners will be asked to provide information on whether any SecureFood partner will further process previously collected personal data. They must also indicate the legal basis for such processing and describe the appropriate technical and organizational measures in place to safeguard the data subjects' fundamental rights.

Here is the question to be presented as an illustration:

Examples of situations in which the controller's interest may be legitimate and permit the processing of personal data: direct marketing, scientific and historical research and the compilation of statistics and, transmitting personal data within the group for administrative purposes.
Legitimate interest is not a valid basis for the processing of personal data by the authorities in the performance of their duties." For more information, see for example the webpage of the Office of the Data Protection Ombudsman, Finland https://tietosuoja.fi/en/controller-s-legitimate-interests or the webpage of the EC https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en

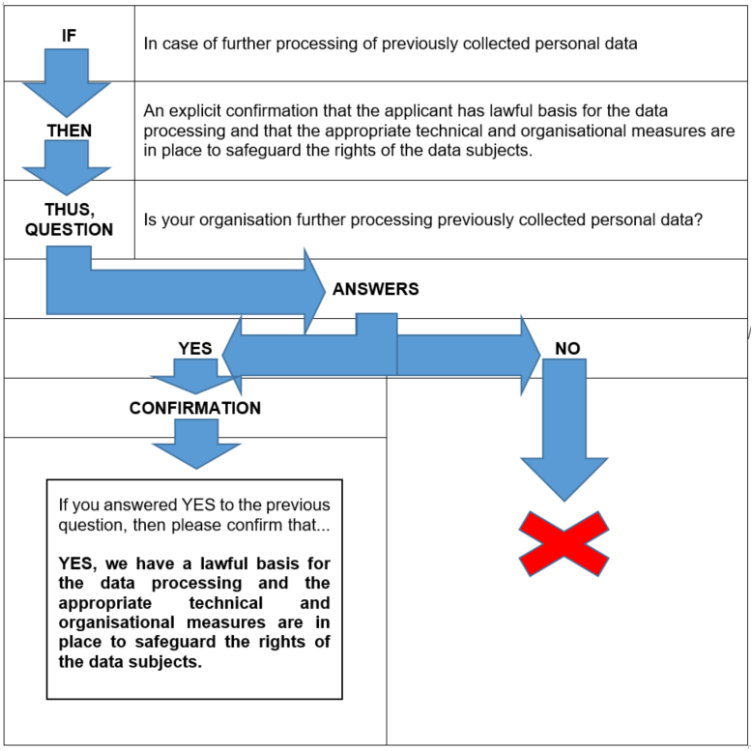

Figure 4-1: Question on further processing

The data will then be collected in a table, see below an example of it (Table 3-2).

Partner	Further processing of previously collected personal data (Yes/No)	If yes, please indicate the legal basis.	If yes, please describe the appropriate technical and organisational measures to safeguard the data subjects' fundamental rights

Table 4-2: Example of data on further processing of previously collected personal data

4.5 Tracking of behaviour and informing the data subjects and safeguarding fundamental rights

Further issue related with personal data is the possible tracking of behaviour and informing the data subjects and safeguarding their fundamental rights. These tracking issues might materialise, for example, in the Living Lab phase of the project, but are not limited to that activity.

The primary concern in ensuring the above is conducting research in an ethically sustainable manner. This includes safeguarding the rights of participants and/or subjects involved in any research. The days when consent was not explicitly obtained, and data subjects were not informed, are long gone.

Again, the consortium members will be asked about this issue too, and the related data will be collected in a form of a table. See here below an example.

Partner	Research involves tracking of behaviour (Yes/No)	If yes, please indicate how the data subjects are informed	If yes, please describe the possible consequences	Measures to safeguard the data subjects' fundamental rights

Table 4-3: Example table of data on tracking of behaviour

4.6 Conclusion on Protecting Personal Data

To ensure the ethical integrity of the SecureFood project, it is crucial to respect the fundamental rights of individuals in the European Union. As explained, a Data Protection Officer (DPO) plays a vital role in ensuring GDPR compliance and safeguarding data subjects' rights. Preventing unauthorized access to personal data is both a fundamental security and ethical issue for SecureFood. Therefore, the consortium members' security measures to prevent unauthorized access will be documented. Anonymization and pseudonymization techniques are ways in this project for protecting personal data too. Also, although further processing of previously collected personal data is unlikely in SecureFood activities, it must be clarified if it occurs. Thus, partners must provide information on further processing, legal bases, and measures to safeguard data subjects' rights. Tracking of behaviour and informing data subjects are also crucial issues, particularly in phases like the Living Lab, requiring explicit consent and transparency. Overall, the primary concern is conducting research in an ethically sustainable manner, safeguarding participants' rights, and ensuring informed consent and transparency in data processing activities.

5 Potential Misuse and Counter-measures

Heavily related to applying the ethical standards presented above is the potential misuse of the research. Thus, this concept of "potential misuse of research" must also be clarified. In our context, it refers to research involving or generating materials, methods, technologies, or knowledge that could be exploited for unethical purposes.

So, what constitutes research and what can be misused? Research, although a relatively abstract term, can be broken down into tangible objects and artifacts, such as machines, devices, and instruments, as well as the infrastructure supporting their use. Additionally, research results can include computing programs, algorithms, and similar outputs. Research often encompasses knowledge in the form of written reports, presentations, articles, and so on. In the case of SecureFood, potential misuse may involve the exploitation of vulnerabilities described in documents produced by SecureFood. Moreover, the term "research" can also encompass the consortium itself and the different ways we interact inside it.

What, then, is misuse for unethical purposes? Unethical purposes typically involve using something beneficial for harmful ends. For example, medical research outcomes like drugs could be misused as illegal substances. Similarly, research in the chemical industry might produce materials that could be used unethically, such as in the creation of bombs from fertilizers. Therefore, the ethical implications of research outcomes are not solely determined by the original purpose or intention. It is crucial to recognize that, even with the best intentions, research outcomes can potentially harm humans, animals, or the environment.

Covering every aspect of unethical uses of research and its findings is challenging, as almost anything can be used ethically or unethically. For instance, a pen, a simple research outcome, could be used to write beautiful poems or sign peace treaties, but it could also be used to write hate speech. Therefore, when considering the potential misuse of research, we narrow down the areas of interest to more manageable categories.

The main areas of concern regarding potential misuse (not in any particular order)[17] according to the Commission's guidance are the following:

1. research providing knowledge, materials and technologies that could be adapted for criminal and/or terrorist activities;
2. research that could result in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery;
3. research involving the development of surveillance technologies that could result in negative impacts on human rights and civil liberties;
4. research on minority or vulnerable groups and research involving the development of social, behavioural, or genetic profiling technologies that could be misapplied for stigmatisation, discrimination, harassment, or intimidation.

Referring to the areas identified in the Commission's guidelines, only the first seems to be realistically relevant to SecureFood. SecureFood focuses on resilience, so naturally research findings in this domain could potentially be misused.

[17] EC, EU Grants: Guidance note — Potential misuse of research: V1.1 — 07.01.2020. Online. Available at: https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf

The second area, although intertwined with the first, seems to be irrelevant, since it is highly unlikely that SecureFood's research could contribute to the development of CBRN (Chemical, Biological, Radiological, and Nuclear) weapons. Even with the relation to e.g., fertilisations that can be utilised in bombs this seems to be too far fetch.

The third and fourth areas are irrelevant to this project for the following reasons: Despite some elements of research on surveillance technologies, SecureFood is not conducting research that could negatively impact human rights and civil liberties. Additionally, SecureFood does not conduct research on minorities or vulnerable groups, nor does it involve profiling technologies. Thus, the research cannot be misapplied for stigmatisation, discrimination, harassment, or intimidation.

Considering the reasoning above, only the first area is worth exploring for potential misuse. The likelihood of any misuse of SecureFood's research findings, criminal or other, is very low.

Above said, the risk is not however non-existent. As one politician has put it:

> *"[…] because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we do not know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones."*[18]

Therefore, whilst there is no specific need to address the misuse question beyond this deliverable, there are counter-measures or specific ways to mitigate this risk too. They will be presented in the next paragraph. The stress of the countermeasures is on mitigating, since all the risks cannot be eliminated, only minimised.[19]

Below are presented the four types of counter-measures designed to prevent the potential misuse of SecureFood research.

1. Ethical Work Throughout the Project: this includes raising awareness of various ethical issues, including misuse, and rigorously following ethics and security guidelines. Ensuring solid ethical practices is fundamental to mitigating misuse risks.
2. Data and Information Sharing Rules: Implementing strict policies and practices for data and information sharing is crucial. For instance, when collaborating on deliverables, partners must correctly use document-sharing protocols and adhere to established document handling rules. Partners are familiar with these practices and follow them diligently. Sensitive deliverables, classified as confidential, are accessible only to the consortium and not publicly available, minimizing misuse risks. Publicly available research results are unlikely to be used for criminal or terrorist activities. These rules are presented in the D1.1.
3. Review Process: Deliverables undergo rigorous review not only for quality but also for ethics and security. This review process helps identify and mitigate potential misuse risks.
4. Partner-Specific Measures: Partners implement various measures to prevent unethical use of SecureFood research. For example, public entities have their own protocols to prevent misuse, which are often confidential and cannot be disclosed in detail. Generally, these measures involve controlling and securing restricted data and information.

Above presented counter-measures collectively help ensure that SecureFood research is conducted and shared responsibly, minimizing the risk of misuse.

[18] Donald Rumsfeld, United States Secretary of Defense at a news briefing on February 12, 2002.
[19] European Commission, Guidance Note – Potential of misuse of research, 07.1.2010, https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf

6 Ethics "Methodology" and future work

This chapter is about how the ethics work is part of the management of the project. First must be emphasised that the ethics work is everyone's obligation: only by ensuring that the work and the outcomes are ethically sustainable and societally acceptable the SecureFood solutions can be certain that they have possibility to become winners in the long run. One could say that ethicalness is one key element of market potential, so therefore, it needs to be kept well and alive during the project too.

The main role of the ethics work is of course handled by the ethics manager. He will compile much of the reporting and sending information requests to the partners, advising, and giving guidance. He will have as an asset a Regulation and Ethics Board (REB), a sort of advisory board that will help analyse and define strategies to ensure that all regulative ethical aspects involving data collection, processing, storage and sharing and research with human participants are fulfilled. In this REB will be present the Ethics Manager, few partners' ethics experts, the Project Coordinator, and the leaders of the pilots.

The work itself will be involving around following key activities that ensures that the project activities are conducted responsibly, respectfully, and in compliance with ethical standards.

1. The utilisation of Informed Consent, i.e., ensuring that all the partners know how ask and get the consent of the participants.
2. Confidentiality and Privacy, ensuring that everyone has the knowledge and means to protect the privacy of participants by keeping their data confidential. This includes data storage, anonymizing/pseudonymisation techniques etc.
3. Risk Assessment: Identifying and minimizing any potential risks to participants. The key here is being involved and having open discussion with the partners on their tasks.
4. Ethical Reviews: When needed the EM and the REB can conduct ethical reviews on the deliverables and other work of SecureFood, so that they meet ethical standards and guidelines.
5. Ongoing Monitoring and Compliance: Continuously monitoring the research process to ensure ongoing compliance with ethical standards. This is mainly done by providing link to a specific ethical self-assessment that aims to pinpoint possible danger areas. The link to the assessment: https://ec.europa.eu/eusurvey/runner/SecureFood_ethics_self_assessment

The results will be reported further to the commission.

6. Transparency and Honesty: One of EM's and REB's task is to promote transparency in the research process, including honest reporting of methods, data, and findings. Researchers should disclose any conflicts of interest and ensure that their work is free from bias. This is done mostly bringing up the issue in e.g., meetings.
7. Respect for Participants: Also reminded in the meetings is the issue of treating all research participants with respect and dignity. This includes being sensitive to their needs, values, and cultural backgrounds, and ensuring that their participation does not lead to harm or exploitation.
8. Ethical Data Management: This is done partly during the preparation of the Data Management Plan, however, EM has its role in it too.
9. Social Responsibility: The considerations of the broader impact of the research on society and the environment are done mainly through the *D8.8 – Societal Impact Report*,

however, the EM has its own role in this, since he is responsible for the D8.8. too. The aim is that researchers will contribute positively and avoid causing harm through their work.

10. Feedback and Communication: One of EM's REB's task is to provide the partners with feedback about the research ethics to ensure that they understand their part in the ethics work. Maintaining open and honest communication with all members throughout the research process in crucial. A link for whistleblowing[20] and/or anonymous inquiries will be created alongside ensuring that everyone has the contact details of the Ethics Manager.
11. Training and Education: this is linked with the above point, since providing ethics training and education for all members of project is key when ensuring that everyone understands and adheres to ethical standards and guidelines.

In addition to the eleven points presented here above, the main thing is perhaps the awareness of the Ethics Manager altogether. The consortium members are regularly approach by different requests and reminders as well as kept aware of ethical issues. This will be most crucial on the future work: getting involved with different activities as well as with all the partners. First, inquiring information on the topics presented in this document, and then discussing and working together with the whole consortium toward common goals. For the first, i.e., the inquiries, a EUSurvey tool questionnaire will be utilised: https://ec.europa.eu/eusurvey/runner/SecureFood_Ethics

All in all: active and regular interaction with the whole consortium is a key for successful ethics work: ethics should not be a burden, rather helping the work.

[20] The project does not officially employ anyone, so SecureFood is not obligated to follow the whistleblowing directive (2019/1937) (https://eur-lex.europa.eu/eli/dir/2019/1937/oj), however, we want to give an mean to reach to the Ethics Manager also anonymously.

7 Annexes

7.1 ANNEX 1: Example of Consent Form

INFORMED CONSENT FORM

FOR PARTICIPATION IN SecureFood ACTIVITIES

Hereby I, ... (first name, last name)

Please clearly mark your selection	YES	NO
I have read the information on this activity, i.e., [add the activity here] of the Horizon Europe funded SecureFood project.		
My questions about the activity have been answered to my satisfaction, and I understand that I may ask further questions at any point.		
I understand that I am free to withdraw from the activity at any time without giving a reason for my withdrawal without any consequences to my future treatment by the researcher.		
I agree to provide information to the activity organisers under the conditions set out here and/or in the *Information Sheet*.		
I have been reassured that after analysis of the minimum information sought and processed, any personal data of mine shall be fully protected and deleted after the conclusion of the study.		
I consent to the information collected for the purposes of this activity, once anonymized/pseudonymised / de-identified/de-linked / (Re)identified (so that I cannot be identified), to be used for any other purposes related to the SecureFood project.		
I wish to participate in the [add the activity here] set out here and/or in the Information Sheet.		

Place:	
Date:	
Participant's signature:	

Should you have any questions, please call or write to the following contact persons	
The person responsible for the [add activity here]:	
Name	[add here]
Organisation:	[add here]
Address:	[add here]
Phone:	[add here]
Email:	[add here]
The Data Controller of SecureFood:	
Name	[add here]
Organisation:	[add here]
Address:	[add here]
Phone:	[add here]
Email:	[add here]
The Coordinator of SecureFood:	
Name	Vassilis Sakas
Organisation:	EUROPEAN DYNAMICS LUXEMBOURG SA
Address:	[add here]
Phone:	[add here]
Email:	vassilis.sakas@eurodyn.com

7.2 ANNEX 2: Example of the Information Sheet

Dear participant,

You are invited to participate in an interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] that is part of the Horizon Europe funded project called SecureFood, Task <number of the Task> that prepares Deliverable(s) <number of the deliverable> and '<title of the deliverable>'
The task Leader is <name and organization of the Task leader>),and it is described in the project's Description of Action as follow: <add full description of the task>.
Before you decide to participate in the present interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one], please, be read carefully the following details and, if you wish, consent to your participation by filling in and signing the attached Consent Form.

What is the SecureFood project about?
The European Union's (EU) Farm to Fork strategy, the Biodiversity strategy and the European Green Deal, lay down important actions that set a long-term vision concerning the change of the way we produce, distribute, and consume food.

In response to these ambitious aims, SecureFood adopts an integrated systems-thinking approach that acknowledges and embraces the complexity of the food supply chain, including all the actors, elements, processes, activities, infrastructure and essential services of importance in the production, distribution and consumption of food in order to maximize the food supply chain resilience.

The goal of SecureFood is to create an ecosystem of scientific knowledge, collaborative processes, and digital tools that will provide evidence-based indications of the risks and vulnerabilities of the different food value categories in different geographies in order to safeguard food security and to ensure that a secure and resilient food supply chain is assured.

The two crucial pillars of the program are the Food Systems Resilience Management Framework with connected resilience and sustainability orientations, as well as a Resilience Governance Framework that draws upon all of the collaborative principles and guidelines of the successful cooperation between the food supply chain stakeholders, which will be created, tested, and demonstrated in real life case studies. These two frameworks will function as applicability and sustainability mechanisms for organizing and adopting the project's results by applying the developed scientific knowledge, and by enhancing the food system resilience at different levels.

The ambition of the program consists of four critical dimensions, which are: 1) the evolution of scientific knowledge and development of the exploratory approach, combining research approach methods that facilitate the risk identification process; 2) the successful safeguarding of the food supply by framing the system resilience and broadening its lens, as well as by assessing and measuring it through a holistic approach which goes beyond national borders and strategies; 3) the acceleration of the transformation of the food systems network, which can be achieved by applying a systematic agency driven collaborative governance approach; 4) and finally, the application of innovative scientific knowledge with the use of advanced digital tools, which will contribute to the successful collection and processing of data sets from several platforms to reshape and redesign the food system trajectory.

The methodology employed is based on three foundational and interconnected elements: the scientific knowledge (existing and developing), the collaborative principles which are dynamically integrated into the methodology, as well the development of digital solutions which will cover all parts of the project (forecasting, statistical analysis etc.). The website of the project is https://secure-food.eu.

Why have you been asked to take part?
You were asked to take part in this research activity due to your expertise and knowledge on the respective matters [or add other reason(s)].
You must be over 18 years old and not be in a situation of any vulnerability due to physical / mental conditions and/or have any perceived obligation to agree. If you are under 18 and/or perceive any pressure whatsoever to take part in this study please do not proceed further as we are not permitted to invite you to participate in this and agree to anything under such circumstances.

What will you need to do?
For the purposes of the research activity, you will take part in the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] as part of <number and name of the task and/or deliverable>. Your contribution will be documented via audio recording / on paper / online [select the correct medium/media].
Any participant's personal data will be anonymised, rendered de-identified or pseudonymised securely. Only the minimum personal data justified as essential for the activity will be asked for, and its use will be strictly limited for the purpose of [insert the legal justification i.e., the purpose here, e.g. communicating personal data within the group for administrative purposes[21]]. All data

[21] For more details, see for example the webpages of the Office of the Data Protection Ombudsman of Finland: https://tietosuoja.fi/en/when-is-the-processing-of-personal-data-permitted and https://tietosuoja.fi/en/controller-s-legitimate-interests

shall be subject to strict Data Protection as planned for and monitored by the Data Controller <insert name and contact details here>.

NB! In case of any automatic data capture (if it is included in the research), it must be disclosed here as well as the legal basis of it].

Where will this take place?
This research activity will take place at <add location (or online)>.

How often will you have to take part, and for how long?
You will take part once / twice… [choose / add correct amount]. Your participation to the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] will take approximately <number> minutes/hours/days/months.

Who will be responsible for all the information when the activity is over?
The responsible of all information, including one on the Consent Form, is the organiser and/or the researcher responsible of the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one]. (See contact details below).

What will happen to the information when the activity is over?
<Add description depending on the specific conditions of each research activity>
The information on the hereby attached Consent Form will be kept securely by the researcher/Data Controller during the lifecycle of the SecureFood project and for a 4-year period after its completion according to the SecureFood Grant Agreement.

How will the SecureFood use my contribution?
As it stated above, the Task Leader / Researcher / <add correct one here> will prepare a specific report and will use participants contributions from the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one]. This report… <add description here>.

How will the SecureFood Consortium deal with incidental findings?
No incidental findings are anticipated during the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one]. However, In case of any incidental findings, SecureFood will follow guidance of the projects Ethical Manager and Security Manager.

How long is the whole SecureFood research likely to last?
The duration of the project is from 1.1.2024 to 30.6.2027.

How can you find out about the results of the study?
The results of the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] will be reported by the Task leader in the context of <number of the deliverable> of the SecureFood Grant Agreement. According to the SecureFood Grant Agreement, this report is [select the correct one] publically available from the project's webpage / confidential, thus, the results are available only amongst the SecureFood Consortium / RESTREINT UE/EU RESTRICTED, thus available only those who have statutory authority.

Are there any foreseeable risks, discomfort or disadvantages that might arise?
There are no foreseeable risks, discomfort or disadvantages. /
There are the following risks…<description of the risks, if any>.

Are there any benefits?
<Add description of the benefits here, e.g. possibility to influence to policy, inform on needs etc.>

When will you have the opportunity to discuss your participation?
This Information Sheet and the attached Consent Form for participation in research will be provided to you before the interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] and you will have time to carefully read them before deciding. You should take sufficient time to consider the invitation and make your decision when you are satisfied that you have fully understood the nature of the research and data processing.
The project website https://secure-food.eu provides more information. However, should you require further clarification please contact the responsible organiser of this interview / survey / questionnaire / workshop [select the correct activity, or add appropriate one] [add contact details here], or the Project Data Controller [add contact details here].

What if you do not wish to take part?
Your participation is totally voluntary. You have the right to entirely or partially refuse to participate and your refusal will not disadvantage you in any way.

What if you change your mind during the study?
In that case, you are free to withdraw your consent to your participation from any part of the present activity at any time, without consequences.
Participant's data can be deleted, subject to the provisions of Art. 17 GDPR, at any time upon request. However, whilst of course we would endeavour to uphold your rights, we may face some restrictions that would apply to the above rights where data is already collected and used for research purposes.

Who is the contact person?
In case you have any questions and concerns or if adverse effects occur after this research activity you can contact<name and contact details of the researcher (both partner/legal entity and the natural person carrying out the research activity>.
For the exercise of your rights related to data protection you may contact <contact details of the DPO> or the researcher.

Your rights in short:
You have the right to file a complaint through your national Data Protection Authority (or by contacting the Data Controller responsible at the address provided above) about any aspect of the conduct of this consent seeking process and of course the right to accept or reject our invitation without any explanation whatsoever. However, if you decide to participate you would continue to have certain rights under the data protection law.
Your rights are:

- Withdraw your consent, for example if you opted in to be added to a participant register
- Access your personal data or ask for a copy
- Rectify inaccuracies in personal data that we hold about you
- Be forgotten, that is your details to be removed from systems that we use to process your personal data
- Restrict uses of your data
- Object to uses of your data, for example retention after you have withdrawn from a study

Please note:
Despite our collective commitment to full compliance assurance with GDPR and local data protection regulations, in the case of any unexpected data breach, were this in anyway to have exposed your data to any privacy protection risks, the respective Data Protection Officer and the Project Data Controller shall be notified in accordance with Articles 33-34-GDPR and you will be formally advised of the data affected and the preventative action taken to ensure that any breaches will be fully investigated to establish cause and prevent recurrences consistent with Art 19, 35, 17.

7.3 ANNEX 3: Example of Data Protection Policy

DATA PROTECTION POLICY

[PARTNER'S NAME] has not designated a Data Protection Officer and is not required to do so neither according to article 37 par.1 GDPR as:
(a) the processing IS NOT carried out by a public authority or body;
(b) the core activities of the controller or the processor DO NOT 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;
(c) the core activities of the controller or the processor DO NOT 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,
nor according to the national data protection legislation.

Therefore, [PARTNER'S NAME] has prepared a detailed data protection policy for the SecureFood project.

(1) NATURE OF PERSONAL DATA:
[PARTNER'S NAME] will process during the lifetime of the Project different types of personal data such as names, e-mails, telephone numbers.
The personal data do not belong to special categories as stipulated in Article 9 GDPR.

(2) PURPOSES OF PROCESSING:
[PARTNER'S NAME] will process personal data for the purposes of the SecureFood Project. The processing is necessary for scientific research 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 subjects.

Particularly, [PARTNER'S NAME] will process personal data:

1. of the personnel of the Consortium Parties for the purposes of communication, interaction, information sharing and management of the Project;
   (the first purpose concerns all the partners)

2. of the research participants during the interviews, surveys and/or the pilots;
   (the second purpose concerns the partners that are going to collect and further process personal information of the participants in the demos and other activities. Hence, delete this if it does not correspond to your role in the project.)

3. included in and exchanged amongst the users via the SecureFood solution.
   (the third purpose concerns the partners that are going to utilise the SecureFood system.

(3) LEGAL BASIS FOR PROCESSING:
The legal basis for processing is the performance of the SecureFood Consortium Agreement and of the SecureFood Grant Agreement with respect to the processing of names, e-mails and telephone numbers of the personnel of Consortium Parties,
(this concerns all the partners)

the informed consent of the participants with respect to the processing of personal data during the pilots
(the second purpose concerns the partners that are going to collect and further process personal information of the participants e.g., in the demos, Living Labs etc. Hence, delete this if it does not correspond to your role in the project.)

and public interest with respect to the personal data included and exchanged via the SecureFood system.
(the third purpose concerns the partners that are going to utilize the SecureFood system).

(4) RECIPIENTS – TRANSFER TO NON-EU COUNTRIES:
Add more recipients if any, e.g., data processor (if personal data will be sent for encryption/anonymization/pseudonymization to a third party), or other third parties/subcontractors if any.

The information will be available amongst the Parties of the Consortium.
The information will be transferred to non-EU countries (partners from Ukraine).
The information may be available to a Party's affiliates / linked third parties.

(5) STORAGE PERIOD:
The personal data will be collected and further processed during the lifetime of the SecureFood project and for a 4-year period after its completion according to the SecureFood Grant Agreement.

(6) SAFEGUARDS: Add more safeguards, if any, and accept the ones in yellow if you are using / going to use such methods.

[PARTNER'S NAME] ensures that both physical and technical measures will be taken for the protection of the personal data which are going to be collected during the lifetime of SecureFood. The safeguards are: the existence of an Ethics Board for the Project,

internal policies, confidentiality agreements, secured storage where only authorized access is allowed, controlled password-protected access to personal computers and to databases containing personal data, privacy by design techniques, encryption, anonymization, pseudonymization.

(7) RIGHTS OF THE DATA SUBJECTS:
Data subjects have the right to:

1. Request information about whether [PARTNER'S NAME] holds personal information about them, and, if so, what that information is and why we are holding it.
2. Request access to their personal information. This enables the data subjects to receive a copy of the personal information we hold about them and to check that we are lawfully processing it.
3. Request rectification of the personal information that we hold about them. This enables the data subjects to have any incomplete or inaccurate information we hold about them corrected.
4. Request erasure of their personal information. This enables the data subjects to ask us to delete or remove personal information where there is no good reason for us continuing to process it.
5. Request the restriction of processing of their personal information. This enables the data subjects to ask us to suspend the processing of personal information about them.
6. Request transfer of their personal information in an electronic and structured form to them or to another party (right to "data portability"). This enables the data subjects to take their data from us in an electronically useable format and to be able to transfer their data to another party in an electronically useable format.
7. Object to the processing of personal data concerning them, on grounds relating to his or her particular situation.
8. Lodge a complaint with a supervisory authority.
9. Withdraw their consent at any time. Once [PARTNER'S NAME] has received notification that the data subject has withdrawn his/her consent, the company will no longer process the personal information for the purpose/purposes the data subject has originally agreed to.

(8) LEGISLATION:
Applicable legislation is the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council 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) and the Law …

For the partners from the EU: Please add your national legislation on the protection of personal data after the GDPR entered into force which has incorporated the GDPR in the national legal framework.

(9) CONTACT:
[PARTNER'S NAME], located in [address], [telephone number], [e-mail address].

[Place], [Date]
[Full name and position in the institution of the person who signs this policy]