Ref. Ares(2023)6615992 - 29/09/2023

holi food

Funded by
the European Union

Legal and Ethical Frame-work

D8.2

Tima Anwana (UNIVIE)
Nikolaus Forgó (UNIVIE)
Katja Hartl (UNIVIE)
Marie-Catherine Wagner (UNIVIE)

September 2023

D8.2

Legal and Ethical Framework

Document ID	D8.2
Due date	30/09/23
Submission date	29/09/23
Dissemination Level	Public
Work Package	8
Author(s)	Tima Anwana (UNIVIE) Nikolaus Forgó (UNIVIE) Katja Hartl (UNIVIE) Marie-Catherine Wagner (UNIVIE)
Document Version	0.5

Grant Agreement	101059813	**Duration**	September 2026
Start Date	October 2022	**End Date**	48 Months

Contributors

Name	Organisation
Tima Anwana	UNIVIE
Nikolaus Forgó	UNIVIE
Katja Hartl	UNIVIE
Marie-Catherine Wagner	UNIVIE

Revision history

Version	Date	Reviewer	Modifications
0.5	29/09/23	Tima Anwana, Katja Hartl	Joint Controllers Modification
0.4	29/09/23	Katja Hartl	Formatting
0.3	29/09/23	Nathan Meijer	Finalization
0.2	28/09/23	Tima Anwana	Update concerning data transfers third countries
0.1	13/09/23	Tima Anwana, Nikolaus Forgó, Katja Hartl, Marie-Catherine Wagner	Draft

Disclaimer: The information and views set out in this report are those of the author(s) 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 herein.

Index of Contents

Index of Tables

Index of Figures

1 Executive summary

This deliverable presents the Legal and Ethical Framework for the EU funded project HOLiFOOD. Desk research methodology has been employed to collect and analyse information from primary and secondary sources. The deliverable aims to provide an overview of the legal and ethical considerations that have an impact on the research activities in the HOLiFOOD project and the overall functioning of the HOLiFOOD platform.

The deliverable explores fundamental rights and their significance in the context of the project. Thereafter, the deliverable focuses on the processing of personal data and the steps implemented in the project to ensure compliance with the GDPR. A key feature of this deliverable is the description of informed consent. To facilitate GDPR compliance, an informed consent form template has been provided by UNIVIE. This form shall be used for the involvement of external stakeholders (added as Annex B). The data protection roles and responsibilities within the project are outlined in this document, and the corresponding Joint Controllership Arrangement is enclosed in Annex A.

In addition to the GDPR, this deliverable addresses the European Data Strategy and upcoming EU legislations such as the AI Act. Furthermore, the European Green Deal and the Farm to Fork Strategy are highlighted as HOLiFOOD tools will contribute to this strategy. Combined with the legal framework, the ethical framework describes the principles for ethical research, AI ethics with regard to the development of the AI component and ethical standards for platforms.

2 Introduction

2.1 HOLiFOOD

The overall objective of HOLiFOOD is to improve the integrated food safety risk analysis (RA) framework in Europe to i) meet future challenges arising from Green Deal policy driven transitions in particular in relation to climate driven changes, ii) contribute to the UN's Sustainable Development Goals and iii) support the realization of a truly secure and sustainable food production. HOLiFOOD will apply a system approach, which take the whole environment into account in which food is being produced, including economic, environmental and social aspects. Three supply chains will be considered (i.e. cereals [maize], legumes [lentils] and poultry [chicken]). Artificial Intelligence (AI) and big data technologies will be used in the development of early warning and emerging risks prediction systems for known and unknown food safety hazards. In addition, tools, methods and approaches will be developed for hazard detection and will be targeted and non-targeted and new holistic risk assessment methods will be develop in which food safety risk will be embedded in a comprehensive cost-benefit analysis of the food system including positive and negative health, environment and economic dimensions. An effective impact pathway will be developed and implemented through integration of the HOLiFOOD outputs into the legal framework associated with the food risk analysis process. The impact pathway will be supported by an electronic data and knowledge sharing platform aiming at the full digitalization of food (safety) systems and supporting transparency and impact for all stakeholders. In order to align with stakeholder priorities, preferences and user requirements, the HOLiFOOD innovations will be designed and tested in a multi actor approach (i.e. Living Lab) involving all stakeholders (e.g. authorities, food producers and citizens).

2.2 Introduction to this document

To achieve the abovementioned objectives the consortium has to adhere relevant laws, regulations and ethical standards. The aim of the Legal and Ethical Framework (D8.2) is to provide the Consortium with guidelines on legally compliant development of the technology and general conduct within the project. This report will provide an overview of the relevant applicable rules and will give an outlook to the possible future legislation concerning data governance, AI and issues related to the EU Green deal.

This report, D8.2 “Legal and Ethical Framework” is the first iteration. The updated and final version will be submitted at the end of the project (M48).

3 Methodology

The methodology used in this report was based on desktop research, including reviews of current and pending legislation and academic commentaries or papers regarding the same. The legal analysis undertaken by UNIVIE has been conducted on European Union (EU) law. This deliverable reflects the main legal and ethical considerations for the HOLiFOOD project after one year. A second iteration of this document, to be submitted at the end of the project (Month 48), will provide a more detailed analysis of the implementation of the legal concepts and laws. This Legal and Ethical Framework deliverable will support HOLiFOOD partners, the project as a whole, and the project coordination team to keep the project fully in line with legal and ethical requirements. Partners, as legal entities, are responsible for ensuring compliance with the relevant legislation addressed in this report.

4 Protection of Personal Data

4.1 Data Protection as Fundamental Right(s)

The Charter of Fundamental Rights (CFR) of the European Union[1] contains the fundamental human rights within the EU, including civil, political, economic and social rights.[2] In the context of the HOLiFOOD project the rights in Article 7, 8, 13 are important. Article 7 of the Charter contains the "right to respect for private and family life". This right also extends to communications. Article 8 of the Charter outlines the "right to protection of personal data". This right protects individuals whenever their personal information is processed and is given effect within the EU through the General Data Protection Regulation (GDPR).[3] Article 13 of the Charter contains the right to freedom of the arts and sciences. As such, scientific or academic research shall be free from restrictions and shall be respected. This Article highlights the importance of scientific research, however, scientific research must be conducted in a manner which is compliant with law and ethics. When dealing with personal data in a research context, none of these fundamental rights prevails in absolute terms over the other. Even more so, the data subject's right to protection of their personal data needs to be balanced with the researcher's right to conduct scientific research.

4.2 Scope and Application of the GDPR

The processing of personal data within the EU is governed by the General Data Protection Regulation (GDPR). The Regulation applies to the processing of personal data by automated and manual means. From a territorial perspective, the GDPR applies to data controllers and data processors that are established within the EU.[4] In certain instances, the GDPR regulates the actions of controllers and processors that are not established within the EU when they monitor behavior, offer goods or services to EU data subjects.[5] Finally, the Regulation applies to non-EU controllers and processors that are established in a place where Member State law is applicable, by virtue of public international law, such as embassies and consulates of EU Member States.[6]

[1] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012.
[2] Equality and Human Rights Commission, 'What Is the Charter of Fundamental Rights of the European Union? | Equality and Human Rights Commission' (Equalityhumanrights.com2010) <https://www.equalityhuman-rights.com/en/what-are-human-rights/how-are-your-rights-protected/what-charter-fundamental-rights-european-union>.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and re-pealing Directive 95/46/EC (General Data Protection Regulation)
[4] GDPR, Article 3(1).
[5] GDPR, Article 3(2).
[6] GDPR, Article 3(3).

4.3 Data Processing

The GDPR broadly defines personal data as “any information relating to an identified and identifiable natural person”.[7] Some examples of personal data include names, identification numbers, location data.The GDPR defines processing broadly as “any operation or sets of operations performed on personal data through automated or manual means”.[8] Some examples of processing operations included “collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure, and dissemination.

In the context of the HOLiFOODs project, the involvement of external stakeholders is foreseen in various Work Packages, ie Living Labs (WP4).

The following stakeholders’ data will be processed:

- name
- e-mail address(es)
- affiliation(s)
- video and audiorecording(s)

This participation requires legal and ethical considerations and appropriate legal agreements and documents, laying down data protection roles and responsibilities among partners.

4.4 Principles of Processing Personal Data

The GDPR establishes a set of fundamental principles that controllers must adhere to when processing personal data to ensure the protection of individuals' rights and freedoms. In the context of an EU funded project, where multiple entities collaborate to process personal data, it becomes imperative to uphold these principles and ensure the protection of personal data, in particular of external parties. Article 5 GPDR sets out the ‘Principles relating to processing of personal data’. These principles apply to all processing activities taking place under the GDPR. Any failure to adhere with the principles set out in Article 5 could lead to an administrative inquiry from the supervisory authority, to financial fines or to civil liability. As such, the following sub-section will outline each of the principles of data protection as set out in the GDPR and explain its implementation in the HOLiFOOD project.

(a) Lawfulness, Fairness and Transpancy

Article 5(1) introduces three fundamental principles: lawfulness, fairness, and transparency. One key requirement of EU data protection is that personal data processing is only allowed when it is based on a specific legal basis. Article 6(1) GDPR sets out an exhaustive list of legal bases and it is the responsibility of the controller to identify and apply the most appropriate legal basis. In the HOLiFOOD project consent in the sense of Article 6(1)(a) GDPR will be the primary legal basis for processing stakeholder data. A detailed description of the process is described below in section 4.5.

The principle of fairness is one that aims at eliminating the imbalance of power between the controller and the data subjects meaning that the data subject should in no way be deceived or confused about the nature of the processing of their personal data. As such, this principle goes hand in hand with the principle of transparency. The controller's responsibilities related to transparency are outlined in Articles 12 to 14 of the GDPR. Article 12 explains how essential information should be communicated to data subjects. Articles 13 and 14 detail what information needs to be communicated to data subjects. In the context of HOLiFOOD data subjects will be informed about their participation in the project and the processing of their personal data (more details in section 4.5).

(b) Purpose limitation

The second principle of data processing under GDPR’s Article 5 is the “purpose limitation.” This principle requires that personal data be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes”. The specificity and explicitly of the processing must be specific enough to prevent the endless reuse of the data and to allow the

[7] GDPR, Article 4(1).
[8] GDPR, Article 4(2).

purposes to be transparently communicated to the data subject in line with Articles 12 to 14. The Working Party 29 (WP29)[9] asserts that "vague or general purposes such as 'improving users' experience', 'marketing', 'IT-security' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'."[10] In the context of the processing for the purposes of scientific research, Article 5(1)(b) states that "further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes".

The scope of the purpose defined in the consent allows partners to contact stakeholders and process their data at various stages of the project without seeking again for their consent. However, the purpose is limited to the aim and scope of the HOLiFOOD project. More details about the purpose for processing the data can be found in the template of the informed consent in Annex B.

(c) Data Minimisation and Storage Limitation

The data minimisation principle means that the controller should only collect and process personal data that is needed for a specific lawful purpose. This purpose should align with the principle of limiting how long data is stored, as mentioned in Article 5(1)(e). This means that the controller must delete personal data once it is no longer needed for the stated purpose. It is the controller's responsibility to have internal processes in place to continuously check if individual pieces of personal data are still necessary for the stated purpose. This duty of the controller is further explained in Article 17 of the GDPR, which talks about the right to erasure.

In the HOLiFOOD project, personal data of stakeholders such as contact details will be stored in a joint repository. In accordance with the purpose set forth in the consent form, the coordinator of the project, WR, will delete data subjects' data upon request (exercise of data subjects' right) and by default after the end of the project (including the final review).

(d) Accuaracy

The accuracy principle of the GDPR requires that data shall be:

> *accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');*

If data is not accurate, then processing may not serve its intended purpose and it may even be detrimental to the data subject. This principle therefore places an obligation on the controller and processor to ensure that the data always are accurate, and that any inaccuracies must be amended in a timely manner. The coordinator, WR, will keep as main contact point for data subjects to keep the data accurate.

(e) Integrity and Confidentiality

Article 5(1)(f) GDPR outlines the principle of 'integrity and confidentiality' in processing, stating that personal data shall be:

> *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*[11]

This principle is elaborated upon in Article 32 GDPR, which details how controllers and processors may adhere to this principle and ensure the overall security of the personal data being processed:

> *1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the*

[9] Article 29 Working Party is predecessor of the European Data Protection Board (EDPB), an independent European body with the aim of ensuring the consistent application of the General Data Protection Regulation and promoting cooperation between EU data protection authorities. On 25 May 2018, the EDPB replaced the Article 29 Working Party.

[10] Working Party 29, Opinion 03/2013 on purpose limitation, WP 203, 02.04.2013, p 52, available at < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>

[11] GDPR, Article 5(1)(f).

rights and freedoms of natural persons, the controller and the processor shall 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.[12]

Article 32 provides examples of the types of security measures that could be implemented. However, this is not an exhaustive list of measures, nor is a definition of the appropriate security measures provided. Rather, controllers must assess the potential risk of processing associated with the type, means and risks to the data subject and ascribe the appropriate security measures. In the HOLiFOOD project, the data will be securely stored on the joint repository using Microsoft Teams. Only Joint Controllers as set out in the Joint Controllership Arrangement (see Annex A) will have access to the relevant data. Microsoft Teams acts as data processor. More details about data security can be found in the Joint Controllership Arrangement (Annex A) and the Informed Consent template (Annex B).

4.5 Informed Consent

Informed consent is an essential building block of research ethics. In order to participate in an EU funded project it is therefore required to seek for an informed consent. The processing of personal data is also based on consent in accordance with Article 6(1)(a) GDPR.

Consent is defined in Article 4(11) as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. The following table highlights the measures implemented in the HOLiFOOD project to ensure that the consent is valid in accordance with Article 7 GDPR.

Condition for Consent	Elements to Consider	In the HOLiFOOD Project
Consent must be freely given:	• Consent should be given by data subject of their own free will; • Data subjects should not be pressured/coerced into giving their consent; • When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.	The participation is voluntary and can be discontinued at any time. Stakeholders are informed about this with informed consent.

[12] Article 32 GDPR.

Consent must be specific	• Consent requests for the processing of personal data must be distinguishable from other requests; • It needs to be clear to the data subject that they are consenting to the processing of their personal data.	Stakeholders are asked to consent to: - participate in the research project - allow the processing of their personal data - not share any of the personal data or business sensitive information disclosed by any third party Each consent is clearly distinguished from each other. Participants are required to check boxes for each element. In order to reduce stakeholder fatigue by asking them for their consent in every interaction, external stakeholders will be asked for their consent to participate in the HOLiFOOD research project and for processing their personal data.
Consent must be informed	Prior to consent the data subject must be properly informed about the intended processing operations and of their rights.	External stakeholders will be informed about their participation in the project and the processing of their personal data. UNIVIE drafted in collaboration with the respective partners an Informed Consent Template (Annex B). Data subjects are informed prior any processing activities. Depending on the form of request data subjects are informed via the website, email or face-to-face.
Withdrawal of Consent	• Data subjects have the right to withdraw their consent at any time. It must be easy for the data subject to withdraw their consent and they should not face any adverse consequences for choosing to withdraw consent. • The withdrawal of consent does not affect the lawfulness of processing that was done prior to the consent. However, continued processing on this basis would be unlawful.	Data subjects are informed about their right to withdraw their consent at any time. The consent can be withdrawn by informing the contact point (the coordinator) or the one of the Joint Controllers named in the informed consent.
Demonstrate Consent	The data controller must be able to demonstrate that the data subject	All consents will be stored by the respective partner. In case of consent collection in the

	has given their consent by maintain records of data subject's consents.	scope of the Joint Controllership Arrangement, the consents will be centrally stored on the HOLiFOOD repository administered by the coordinator (WR). Data subjects are informed accordingly.

Table 1: Conditions for Consent under GDPR and its implementation in the HOLiFOOD project

The consortium will include a registration form on the website including the informed consent. However, some processing activities will require specific processes to involve stakeholders and consequently collect the consent. For example, in WP5 it is foreseen to involve (large) groups of citizens through surveys and interviews. The informed consent will be translated in the respective language and collected and stored by selected partners. Furthermore, a citizen science app will be used. UNIVIE assists relevant partners to ensure legal and ethical compliance in these cases and will report in the updated versions of the DMP (M24, M48) and the second iteration of the legal and ethical framework (M48).

4.6 Data Protection Roles and Responsibilities

The GDPR defines various actors in a personal data operation. The following table provides an overview of the three main actors in the processing activities foreseen in the HOLiFOOD project.

	Definition	Roles in the HOLiFOOD Project
Data Subject	The natural person/individual to whom the personal data being processed is related. The natural person/individual that can be identified or identifiable in relation to the personal data in question (Article 4(1)).	In different workpackages (WPs), it is foreseen to involve external stakeholders (experts and citizens) in different ways (e.g. focus group calls, living labs and surveys). This involvement results in processing of personal data such as contact details of the stakeholders.
Data Controller/Joint Controllers	The entity which alone and jointly determines the purposes and means of processing personal data. The controller(s) determines the key aspects regarding the processing operations. Where two or more controllers jointly determine the purpose and means of processing, they are referred to as joint controllers.	Generally, each partner is solely responsible to ensure compliance with EU regulation as well as national law. However, in order to facilitate the collaboration between partners in HOLiFOOD, selected partners concluded a Joint Controllership Arrangement pursuant to Article 26 GDPR (see Annex A). Each Controller is represented by a PI. In accordance with the GDPR, the Arrangement enters into force at the date of the agreement and confirmation of each party by its PI via e-mail. All amendments to this Arrangement will also be concluded electronically via email. The agreed draft of the arrangement is attached to this deliverable (Annex A).

		In accordance with Article 26 GDPR, the data subject will be provided with all necessary information about the Joint Controllership Arrangement including a point of contact from each institution. However, in order to facilitate the process, data subjects are provided with one single contact point, namely the coordinator of the HOLiFOOD project. This allows data subjects to exercise their rights in an easy way.
Data Processor	The entity which processes personal data on behalf of the controller(s).	Microsoft Teams acts as Data Processor for storing personal data i.e. contact details of external stakeholders

Table 2: Actors according to the GDPR in the HOLiFOOD project

5 European Strategy for Data and Proposed Legislations

In 2020, the European Data Strategy laid out a plan for creating a unified data market in Europe, with a strong focus on promoting reliable and transparent data systems, ensuring fairness, and empowering individuals. The Strategy seeks to establish a single market for data to enhance Europe's global competitiveness and maintain data sovereignty. Through the creation of shared European data spaces, greater data availability for economic and societal purposes is ensured, all while preserving the control of data generators, including companies and individuals. In line with these policy objectives, the European Union has enacted the Data Governance Act, aimed at fostering the establishment of data hubs within critical sectors of the EU economy. Additionally, the European Commission adapted the Data Act in 2022. The overarching goal is to eliminate obstacles to data access, benefiting both consumers and businesses.

The following sub-sections outlines the scope of each legal act and briefly discuss its potential impact on the HOLiFOOD project. A more detailed analysis will be provided in the updated version of this deliverable at the end of the project. However, the legal and ethical helpdesk team (T8.4) will monitor current developments and advise partners accordingly in the course of the project through workshops, calls and guidelines circulated via e-mail whenever necessary.

5.1 Data Governance Act

An integral component of the European data strategy, the Data Governance Act (DGA) aims to increase trust in data sharing, enhance mechanisms for expanding data accessibility, and surmount technical hurdles related to data reuse. Furthermore, the DGA's objective is to facilitate the establishment and growth of shared European data ecosystems in critical sectors. This collaborative effort will engage both public and private stakeholders across domains such as healthcare, environmental conservation, energy, agriculture, transportation, finance, manufacturing, public administration, and workforce development. As of June 23, 2022, the Data Governance Act has come into effect. The Act will apply from 24 September 2023.[13]

The DGA aims at providing a harmonised legal framework for data re-use in connection with other EU and member state laws. The DGA governs the re-use of publicly held protected data with an aim of increasing the availability of such data. It also aims to facilitate data sharing through the regulation of

[13] DGA Article 38.

data intermediaries and by encouraging the sharing of data for altruistic purposes. The DGA encompasses both personal and non-personal data; in the case of the former, the GDPR applies.[14]

While the DGA is crucial for promoting data sharing and transparency in specific contexts, it may not directly apply to HOLiFOOD. HOLiFOOD's research output, focuses on food safety risk analysis and sustainability in food production, which does not align directly with the Act's central objectives related to data sharing. However, HOLiFOOD, which relies on data analysis and research, can leverage this framework to access valuable data from various sources, including public and private sectors, which can enhance the quality and scope of its research.

5.2 Data Act

The proposed Regulation on harmonised rules for fair access to and use of data – also known as the Data Act – was adopted by the Commission on February 23, 2022. A central focus of the Data Act is to ensure fairness by setting out rules for the use of data generated by products and related services. According to Article 2(2) Data Act a 'product' "means a tangible, movable item, including where incorporated in an immovable item, that obtains, generates or collects, data concerning its use or environment, and that is able to communicate data via a publicly available electronic communications service and whose primary function is not the storing and processing of data". In the case of the HOLiFOOD project, the outputs and outcomes are not in the form of tangible, movable items that align with the criteria set out in Article 2(2) of the Data Act. Instead, the project's focus lies in systemic improvements to food safety risk analysis, the development of tools and methodologies, and the integration of outputs into the legal framework of the food risk analysis process.

6 Artificial Intelligence and Big Data Analytics

6.1 EU AI Act

The HOLiFOOD project implements AI to improve the integrated food safety risk analysis (RA) framework within Europe. As a result, this section of the deliverable provides an overview of the EU's proposed AI Act and the implications on the HOLiFOOD project. The proposed Artificial Intelligence Act[15] (AI Act) outlines the approach towards the regulation of AI within the EU. The Act aims to protect individuals by establishing and harmonsing rules for the use of AI systems within the Union. To achieve these objectives, the Act adopts a risk based approach by designating three risk categories for AI systems.

Although it is the topic of much conversation, the AI Act is still in the proposal phase and has not yet entered into force. This deliverable focuses on the current version of the proposed Act which was endorsed by the European Parliament on June 14 2023. Negotiations between the Council, Parliament and the European Commission on the final version of the Act are set to commence. Once officially adopted into law, the AI Act will be applicable in all Member States, this is expected to occur by the end of 2023.

6.2 Subject Matter and Scope

The current version of the proposed AI Act deals with the following subject matter, as outlined in Article 1.

(a) Harmonising rules for the placing on the market, the putting into service and the use of AI systems within the Union;
(b) Prohibitions of certain AI practices;

[14] European Commission. "Data Governance Act Explained", https://digital-strategy.ec.europa.eu/en/policies/data-governance-act explained#:~:text=The%20Data%20Governance%20Act%20(DGA,of%20data%20for%20altruistic%20purposes. (Accessed 10 April 2023).
[15] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS.

(c) Outlining the requirements for high-risk AI systems and obligations for operators of such systems;
(d) Harmonising transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;
(e) Establishing rules on market monitoring and surveillance.

Once enforceable, the AI Act will apply to providers of AI systems within the EU regardless of where they are established (in the union or in third countries)[16] and to users of AI systems within the EU.[17] The Act will also have extra-territorial application as it applies to providers and users of AI systems that are located in third countries, where the output produced by the system is used in the Union.[18] In this context, the following definitions are applicable:

- Provider - "natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge";[19]
- User - "any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity";[20]

6.3 Definition of AI

The proposed AI Act defines artificial intelligence systems as a "software that is developed with one or more of the techniques and approaches listed in Annex I of the Act and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".[21] Annexure 1 of the Act outlines the following AI techniques and approaches which fall within the scope of the definition:

(a) "Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning";[22]
(b) "Logic and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems";[23]
(c) "Statistical approaches, Bayesian estimation, search and optimisation methods".[24]

6.4 Regulating AI Systems

The proposed AI Act adopts a risk based approach towards the regulation of AI systems and places obligations based on the extent of the risk proposed by the system. As such, the Act divides AI systems into four risk categories as depicted in Diagram 1.

[16] AI Act, Article 2(1)(a).
[17] AI Act, Article 2(1)(b).
[18] AI Act, Article 2(1)(c).
[19] AI Act, Article 3(2).
[20] AI Act, Article 3(4).
[21] AI Act, Article 3(1).
[22] AI Act, Annex 1(a).
[23] AI Act, Annex 1(b).
[24] AI Act, Annex 1(c).

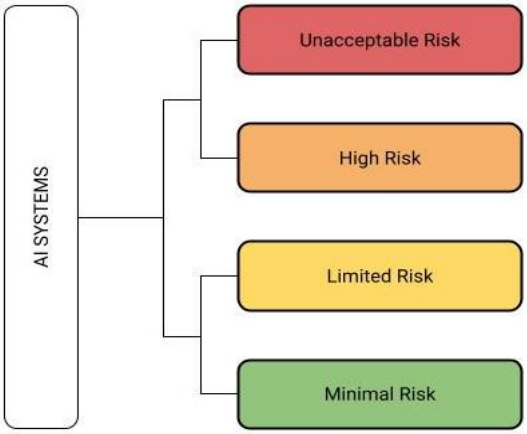


Diagram 1: AI Risk Categories

6.5 Unacceptable Risk and Prohibited AI Practices

The Act prohibits AI systems that pose an "unacceptable risk" to the safety, livelihood and rights of people. Article 5 outlines the following prohibited AI practices and systems.

(a) Cognitive Behavioural Manipulation:

The Act prohibits AI systems which use concealed techniques beyond a person's consciousness in order to significantly alter a person's behaviour in a manner that causes or could potentially cause physical or psychological harm.[25] Furthermore, the Act prohibits AI systems which take advantage of a specific group on the basis of their age, physical or mental disabilities in a manner which alters behaviours and could potentially cause physical or psychological harm.[26]

(b) Social Scoring:

The Act prohibits AI systems implemented by public authorities for the purposes of evaluating or classifying the trustworthiness of natural persons over a period of time. As such, public authorities are prohibited from using AI systems in order to rank natural persons or impose social scores. This prohibition is applicable when such a classification results in the unfair treatment of natural persons or societal groups and this treatment is unjustified to their social behaviour.

(c) Real-time and remote biometric identification systems:

The Act prohibits law enforcement agencies from using 'real-time' biometric identification in public areas. For example facial recognition. However, this prohibition does not apply in certain instances such as for the targeted search of potential victims or missing children, prevention of an imminent threat or a terrorist attack and in the context of criminal offence. The Act further elaborates on the processes to be followed in order to justify the use of real-time biometric identification systems in public areas (see further in Article 5(2)(3) and (4)).

6.6 High Risk AI Systems

The AI Act distinguishes between unacceptable risk and high risk. The use of AI systems that are classified as 'high-risk' is not prohibited, however the Act establishes requirements for high risk AI systems and places specific obligations on users and providers of such systems. High risk AI systems are divided into two categories.

[25] AI Act, Article 5(1)(a).
[26] AI Act, Article 5(1)(b).

The first category of high risk AI systems are those which are used in products falling under the EU's product safety legislation. In such instances, the AI system is classified as high risk when both of the following conditions as depicted in the Diagram 2 below are fulfilled.

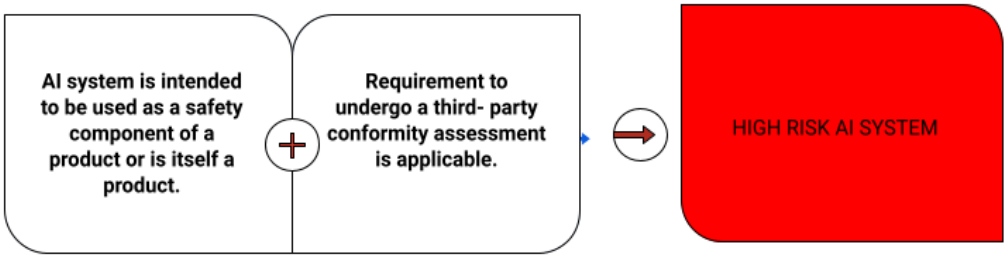


Diagram 2: High Risk AI Systems

The AI system in question is a product or intended to be used as a safety component of a product. Article 3(14) defines a safety component as "a component of a product or of a system which fulfils a safety function for the product or system or the failure or malfunction of which endangers the health and safety of persons or property". Finally, the AI system or safety component is required to undergo a third party conformity assessment (further discussed in the section below).

The second category of high risk AI systems are those which fall into the eight specific areas that are listed in Annex III of the Act.[27] AI systems which are intended to be used in eight areas outlined in the table below shall be classified as high-risk AI systems.

High Risk AI System	Description
Biometric Identification and Categorisation of natural persons.	• This relates to the 'real-time' and 'post' remote biometric identification AI systems.
Management and operation of critical infrastructure	• This relates to AI systems that are to be used as safety components in the context of road traffic, water supply, gas supply.
Educational and Vocational Training	This relates to AI systems used for the following purposes: • To determine access or assign natural persons to education and vocational training institutions; • To assess students in education and vocational training institutions; • To assess participants in tests that are necessary for admission to educational institutions.
Employment, workers management and self employment	This relates to AI systems used for: • Recruitment and employment purposes;

[27] https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_advertiser=Webcomm&at_audience=%7bkeyword%7d&at_topic=Artificial_intelligence_Act&at_location=AT&gclid=CjwKCAjwrranBhAEEiwAzbhNtQ-6cfdw2ys7kcxfnhJq3d3j6oK-pRtSmF0EmwgC4nZ1anVyzxnZwZRoCbHkQAvD_BwE.

	• Advising vacancies, evaluating candidates determining promotions or terminations in the context of employment relationships, task allocation, monitoring performance and behaviours.
Access to essential public services and benefits	This relates to AI systems used to: • Evaluate the eligibility and creditworthiness or similar analysis of a natural person; • AI systems used to dispatch, or to establish priority in the dispatching of emergency first response services.
Law enforcement	This relates to AI systems used: • In the context of law enforcement that may have an impact on the fundamental rights of natural persons; • Conduct risk assessments of natural persons; • Detect the emotional state of a natural person; • Detect deep fakes; • Evaluate evidence; • To make predictions based on profiling of natural persons and to assess personality traits.
Migration, asylum and border control	This relates to AI systems used: • In the context of immigration control, accessing risk, examining applications and verifying the authenticity of travel documents.
Administration of democratic processes	• For example, AI systems which interpret facts and the law and apply the law to a concrete set of facts.

Table 3: AI High Risk Systems

Legal Requirements for High Risk AI Systems

The AI Act imposes certain obligations on providers of high-risk AI systems. These obligations aim to mitigate the risks posed by high-risk AI systems. These obligations relate to:

- Risk management systems (Article 9)
- Data quality and data management (Article 10)
- Draw up and maintain technical documentation (Article 11)
- Record keeping (Article 12)
- Transparency and the provision of information to users of high risk AI systems (Article 13)
- Human oversight (Article 14)
- Accuracy, robustness and cybersecurity (Article 15)

The following steps need to be followed in order to lawfully bring a high risk AI system onto the market for the use of consumers.

Step 1: Identification
The AI system in question must be accessed to determine whether it fits within the definition and classification of a high risk AI system.

Step 2: Conformity Assessment
Conduct a conformity assessment to demonstrate compliance with the requirements of Chapter 2 and Title III of the AI Act, relating to high-risk AI systems. This assessment must be performed before placing the AI system on the market or putting the system into service.

Step 3: Notification
The national notifying authority, in the Member State must be notified and verify the conformity of the AI system.

Step 4: CE Marking of Conformity
Declaration of conformity is signed and the CE mark is placed on the AI system.

Step 5: Registration
The high risk AI system is registered in an EU database and can be placed on the market or put into service.

6.7 Limited Risk AI Systems

Limited Risk AI systems do not pose an immediate threat on the rights and freedoms of natural persons. Some examples of limited risk AI systems include Chabot's, deep fakes, emotion recognition systems and biometric categorisation systems. However, the AI Act does impose some specific transparency requirements on providers of limited risk AI systems. These requirements are outlined in Article 52 of the AI Act. Natural persons must be informed that they are interacting with an AI system or with AI generated content. The obligation to inform natural persons that are interacting with an AI system does not apply in two instances:

(a) To AI systems or the use thereof that is authorised by law in the context of criminal prosecution.
(b) When the use of AI systems is necessary for the exercise of the rights to freedom of expression and the right to freedom of the arts and sciences, subject to safeguards being implemented.

6.8 Minimal or no Risk AI Systems

The proposed AI Act allows the free use of minimal or no risk AI systems with no clear obligations imposed. The Commission provides the following examples of minimal risk systems: video games or spam filters.

6.9 AI and the HOLiFOOD Project

The HOLiFOOD project implements AI to improve the integrated food safety risk analysis (RA) framework within Europe. Artificial Intelligence (AI) and big data technologies will be used in the development of early warning and emerging risk prediction systems for known and unknown food safety hazards. As a result, the technologies to be used in the project fall within the ambit of the proposed AI Act.

The AI systems used in the project can be classified as Limited Risk AI Systems. This classification is suitable as the AI systems in the project do not pose an immediate threat to the rights and freedoms of individuals nor does it fall within the predefined categories of high-risk AI systems in Annex III of the Act. Instead these systems are used to provide early predictions in the context of food safety hazards in order to protect actors in the food supply chain. As such, the project would be required to adhere to certain transparency requirements outlined in Article 52 of the proposed AI Act. In accordance with Article 52(1), AI systems which are intended to interact with natural persons shall be developed in a way which ensures that the users are informed that they are interacting with an AI system. Therefore, it must be made clear to the users of the HOLiFOOD tools when predictions for food safety hazards are made using AI systems.

7 EU Green Deal with a Focus on the Farm to Fork Strategy

7.1 The European Green Deal

The European Green Deal represents a profound commitment by the European Union to address urgent environmental challenges and foster sustainable development. Since its introduction in 2019, several key policies and initiatives have been implemented to advance its goals:

1. **Climate Law:** The EU's climate law enshrines the commitment to achieve climate neutrality by 2050 into legislation. It sets a legally binding target of reducing net greenhouse gas emissions by at least 55% by 2030 compared to 1990 levels.

2. **Renewable Energy:** The EU has increased its renewable energy targets, aiming for 32% of energy consumption to come from renewable sources by 2030. This involves substantial investment in wind, solar, and hydroelectric power infrastructure.
3. **Circular Economy Action Plan:** To promote sustainability and reduce waste, the EU has launched an action plan focused on creating a circular economy, which includes measures to improve resource efficiency and promote recycling.
4. **Biodiversity Strategy:** The EU's biodiversity strategy aims to protect and restore biodiversity, including setting a goal to protect 30% of EU land and sea areas by 2030.
5. **Farm to Fork Strategy:** This strategy aims to make European food systems more sustainable, ensuring healthy food production while minimizing the environmental impact.
6. **Just Transition Mechanism:** Recognizing the potential socio-economic impacts of the transition, the EU has established a Just Transition Mechanism to support regions and sectors heavily dependent on fossil fuels to shift towards cleaner alternatives.

7.2 The Farm to Fork Strategy

The Farm to Fork Strategy[28], a key component of the European Green Deal, specifically targets the food system. It acknowledges that the food production and consumption cycle significantly affects environmental, health, and societal outcomes. The strategy aims to create a sustainable food system by promoting healthier diets, reducing the environmental impact of food production, enhancing food safety, and supporting rural economies. It emphasizes the need to align food production with environmental sustainability, human health, and animal welfare. Consequently, this section mainly explains the goals and aims of the Farm to Fork Strategy and how HOLiFOOD contributes to its implementation. Key objectives and elements of the Farm to Fork strategy include:

1. **Sustainable Food Production:** The strategy seeks to make European food production more environmentally friendly by promoting practices that reduce the use of pesticides and antibiotics, increase soil health, and enhance biodiversity on farms.
2. **Reduction of Chemical Pesticides and Fertilizers:** The strategy aims to reduce the use and risk of chemical pesticides and fertilizers by setting targets for their reduction, while also promoting the use of integrated pest management and organic farming practices.
3. **Promotion of Organic Farming:** The strategy encourages the expansion of organic farming practices in the EU to promote more sustainable and environmentally friendly agricultural systems.
4. **Animal Welfare:** The strategy emphasizes improving animal welfare standards, including better living conditions and reduced use of antibiotics in animal farming.
5. **Food Labeling and Transparency:** The strategy aims to enhance consumer information and awareness by introducing mandatory front-of-pack nutrition labeling and other measures to provide accurate information about the nutritional content of food products.
6. **Promotion of Healthy Diets:** The strategy seeks to encourage healthier eating habits among Europeans by promoting the consumption of fruits, vegetables, whole grains, and sustainable proteins.
7. **Reduction of Food Waste:** The strategy sets a goal to reduce food waste across the food supply chain, from production to consumption, and promote measures to limit food losses.
8. **Research and Innovation:** The strategy highlights the importance of research and innovation in developing and implementing sustainable agricultural and food production practices.
9. **International Cooperation:** The Farm to Fork Strategy recognises the global nature of food systems and aims to promote sustainable food production and consumption beyond the EU's borders through international cooperation.

By addressing the entire food supply chain, from production to consumption, the Farm to Fork Strategy seeks to create a more resilient, sustainable, and equitable food system that contributes to a healthier population and a healthier planet. It recognises the need for a comprehensive approach involving stakeholders from various sectors, including agriculture, food industry, health, and environmental conservation.

[28] European Commission, A Farm to Fork Strategy for a fair, healthy and environmentally-friendly food system (2020).

HOLiFOOD acknowledges the complexities linked with the policies of the Green Deal and intends to apply artificial intelligence and extensive data analysis to formulate a holistic approach that accounts for the intricate context in which food production takes place.[29] The use of artificial intelligence (AI) and big data analytics within the HOLiFOOD project aligns with and enhances the implementation of the Farm to Fork Strategy in several key ways. The project's focus on identifying and addressing emerging food safety risks of chemical and biological nature (ERIs) within the food production system connects to the Farm to Fork Strategy's goals of enhancing food safety, reducing environmental impacts, and promoting sustainable agricultural practices. Taking into consideration the overarching goals and aims of the strategy, the HOLiFOOD tools and approaches contribute to the Farm to Fork Strategy by:

HOLiFOOD Tools and Approaches contributing to the Farm to Fork Strategy	
Enhanced Risk Identification	AI and big data analytics enable the HOLiFOOD project to systematically and comprehensively identify both current and potential future ERIs. By analysing vast amounts of data, these technologies can detect trends, anomalies, and patterns that might indicate emerging risks related to food safety and environmental impact. This aligns with the Farm to Fork Strategy's objective of ensuring a safer and healthier food supply.
Holistic System Approach	The Farm to Fork Strategy emphasizes a holistic approach to food systems, considering the interconnectedness of various factors. AI and big data analytics enable HOLiFOOD to implement this system approach effectively. These tools can analyse multifaceted data sets to understand the complex interactions between factors like agricultural practices, environmental conditions, and biological factors. This supports the creation of a sustainable and resilient food system.
Early Detection and Mitigation	By applying AI and big data analytics, the HOLiFOOD project can detect emerging risks at an early stage. Issues can be identified and prevented before they escalate, ensuring timely responses to potential threats to food safety and environmental sustainability. This capability enhances risk reduction and proactive management.
Collective approach	The Farm to Fork Strategy acknowledge that the transition to sustainable food systems requires a collective approach involving public authorities at all levels of governance (including cities, rural and coastal communities), private-sector actors across the food value chain, non-governmental organisations, social partners, academics and citizens. HOLiFOOD's establishment of virtual Living Labs involves engaging stakeholders from diverse geographical and governance backgrounds, promoting multi-level collaboration and aligning with the strategy's goals.
Accessibility to relevant Stakeholders	The integration of the developed ERI system within a knowledge exchange platform (developed in WP6) ensures that the insights and data generated are accessible to relevant stakeholders. This platform facilitates the exchange of information between researchers, risk managers, risk assessors, and other actors involved in the food supply chain. Such collaboration and information sharing are integral to the Farm to Fork Strategy's principles of cooperation and stakeholder engagement.

Table 4: HOLiFOOD tools and approaches contributing to the Farm to Fork Strategy

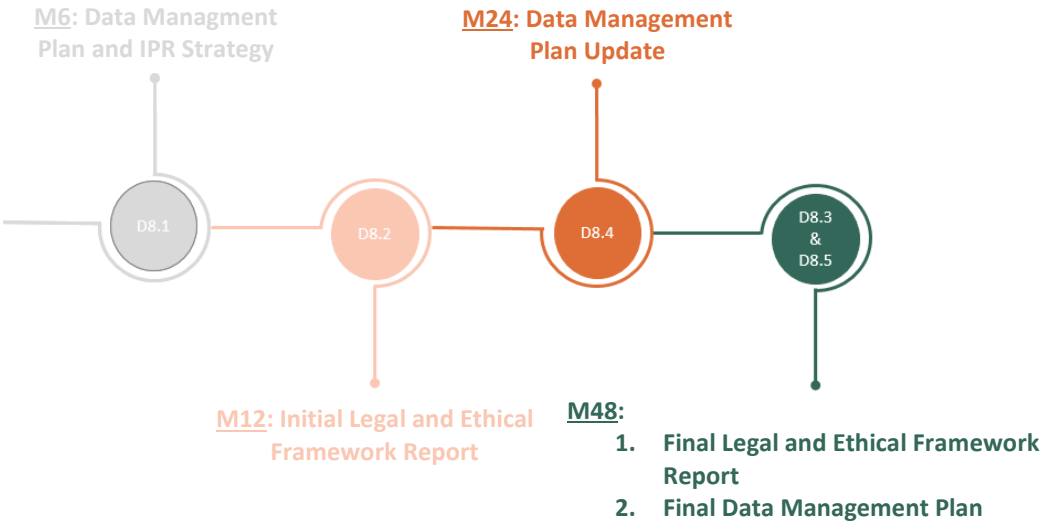
[29] HOLiFOOD Grant Agreement, Part B - p 10.

In summary, the application of AI and big data analytics in the HOLiFOOD project aligns with and advances the objectives of the Farm to Fork Strategy by identifying emerging risks, implementing a holistic approach to risk assessment, enabling early detection and mitigation, and facilitating information exchange among stakeholders. These technologies contribute to a safer, more sustainable, and transparent food system in line with the overarching goals of the EU's Farm to Fork Strategy.

8 Ethical Framework

In addition to legal considerations, it is also essential for research projects such as HOLiFOOD to ensure ethical compliance. Ethical obligations and considerations in the HOLiFOOD project mainly stem from the Ethics Guidelines for Trustworthy AI issued by the High Level Expert Group on AI (HLEG)[30], Article 14 of the Grant Agreement, and widely recognised interdisciplinary ethical principles,[31] some of them ingrained in law.

HOLiFOOD aims to implement the highest standards of ethical research and responsible scientific practice, also to contribute in the development of new approaches to ethical discourse and stimulate debates about ethical scientific practice. Ethics in HOLiFOOD will be guided by WP8 and WP9. WP9 lead by WR coordinates the day-to-day project management including its ethics, and collaborate closely with WP8. WP8 provides assistance and guidance to partners on their project-related matters in their deliverables. D8.1 (DMP) reflected a first evaluation of ethical problems that may arise during the project. A continuous evaluation of the ethical framework and the monitoring of ethical issues will be done through the Ethical Helpdesk set up by WP8. Partners can reach out to the e-mail holifood-helpdesk.id@univie.ac.at with all ethical questions. The Legal and Ethical Helpdesk supports partners in remaining compliant with all ethical requirements. The key ethical requirements will be reflected in this deliverable D8.2 and a final assessment will be provided in D8.3 (Final Legal and Ethical Framework Report) due in M48. In particular, D8.3, D8.4 and D8.5 (DMP I and DMP II) due in M48, M24 and M48 will reflect the ethical challenges that have emerged in HOLiFOOD over time.



8.1 Principles of Ethical Research

Partners involved in HOLiFOOD must respect some fundamental ethics principles. It is the partners' responsibilities to ensure ethical compliance. However, we as legal and ethical helpdesk will assist partners in all possible ways: by providing guidelines (such as this deliverable), address inquiries via email and participate in WP and PMT calls, as well as in one-to-one discussions. To ensure partners

[30] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.
[31] E.g. Concept of Objectivity, Informed Consent, and Anonymization Procedures

respect for ethical principles a self-asssesment questionnaire will be distributed by the beginning of 2024 and assessed in an internal meeting.

Whilst ethics principles may differ between the countries, some ethical standards must be met in order to avoid exclusion from the project or any suspension of payment as described in the Grant Agreement.[32] This includes meeting the highest possible standards of quality, accuracy and transparency in the processes and results of the project. Unacceptable practices are, for example:

- the manipulation of data
- the manipulation of data representations or consents
- the suppression of relevant findings
- the misappropriation of ideas or intellectual property
- the misrepresentation of material interests or conflicts of interest.

HOLiFOOD is committed to sharing its results within and outside the scientific research community, in line with the FAIR principles, which are described detailed in the DMP while always balancing the accessibility against the rights of individuals and other considerations, such as IP rights. Moreover, it should be considered that, while legal and ethical frameworks often converge, not all ethical requirements are codified in law and should therefore be considered in combination with, but distinctly from the legal framework.

8.2 AI Ethics and the Development of the AI Component

In April 2019, the AI HLEG, which is an independent expert group set up by the European Commission published the Ethics Guidelines for Trustworthy AI.[33] These guidelines are a legally non-binding document that contains recommendations for the development of trustworthy AI. The seven ethical requirements that AI systems need to meet in order to be trustworthy are:

1) Human agency and oversight
2) Technical robustness and safety
3) Privacy and data governance
4) Transparency
5) Diversity, non-discrimination and fairness
6) Social and environmental well-being
7) Accountability

In the following paragraphs these seven requirements and possible approaches for implementation in the HOLiFOOD project will be futher discussed. In July 2020 the HLEG established an Assessment List for Trustworthy AI, which is a self-assessment checklist that provides practical tools for the developers and deployers of AI to implement the Ethics Guidelines.[34] The second iteration of this deliverable to be submitted in M48 will reflect the best practices applied in HOLiFOOD.

1) Human agency and oversight

Human agency refers to the impact that AI systems can have on human behavior and helps ensuring that an AI system does not undermine human autonomy or causes other adverse effects. AI systems are often aimed at guiding or supporting humans in decision-making. Human oversight therefore addresses the necessary oversight measures, which need to be self-assessed by partners throughout the project as potential risks arise from changes in data sources, to guarantee human autonomy. Whenever less human oversight becomes possible, stricter governance measures are required.

Before the AI system is generated, it needs to be determined whether it is a self-learning system and is overseen by a Human-in-the-loop, Human-on-the-loop or Human-in-command to guarantee human oversight. Besides this determination it is also equally necessary that training materials for the exercise

[32] GA, p.56
[33] High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019.
[34] High-Level Expert Group on Artificial Intelligence, Assessment List for Trustworthy Artificial Intelligence (AL-TAI) for self-assessment, 2020, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

of oversight measures are available. To avoid confusion of end-users or subjects, awareness that the detection of a food safety risk was detected by the AI system is necessary. Stakeholders and end-users need to be informed that they are interacting with an AI system. Human autonomy must be respected in a way that procedures are put into place that end-users will not over-rely on the AI system by going against their own non-automatically created results.

2) Technical robustness and safety

AI systems must be developed with a preventative approach to fulfil the second requirement, which consists of the following four sub-components:

- Resilience to attack, and security;
- A back-up plan and general safety;
- Accuracy;
- Reliability and reproducibility.

Vulnerabilities within the AI system may cause a wide range of damage, when the system can be likely attacked by e.g. hackers. Therefore, it is crucial that providers of AI systems implement safety measures from the very beginning and also establish back-up safety plans. AI systems should be able correct recommendations and also change their considerations. To fulfil reliability a well-described process to monitor whether the AI system is meeting the intended goals should be defined.

3) Privacy and Data Governance

Firstly, this requirement concerns privacy and data protection as it is enshrined in law and described above in the legal section. This means that unlawful data processing must be avoided throughout the lifecycle of the AI system, not only during the project. Secondly, it is crucial that the data are accurate, sufficiently broad and representative and are not containing any socially constructed biases or inaccuracies. During data collection, this should be considered and discriminatory bias should be removed or counteracted where possible. Thirdly, the access to the data is described in detail in the Joint Controllership Arrangement, prepared by WP8.

Although in HOLiFOOD the data processed is mostly non-personal data, the privacy and data protection implications of the AI system should still be considered for non-personal training-data or any other processed non-personal data. To ensure data protection by design and default this should kept in mind in all developing stages.

4) Transparency

The requirement of transparency refers to AI systems, the data and AI business models and consists of three sub-components: - traceability, - explainability and - communication about its limitations. Traceability mechanisms, which can point to the reasons for an error in an AI system, achieve transparency. Humans need to be aware when they are interacting with an AI system, and the decisions made by AI systems must be explainable to the stakeholders concerned (see already human oversight). The complexity of AI systems can lead to a “black-box-problem”, where errors are difficult to identify and responsibility is difficult to allocate, therefore there must be a focus on transparency.

Making AI explainable means putting technical details into a format that humans find comprehensible to some degree.[35] Even where trade-offs may have to be made between accuracy and explainability, it is key that humans should be able to understand the information generated by AI. Explainability is also overlapping with the third component, which is communication. Informing stakeholders, end-users and subsequently the general public can help in raising awareness about the fact that AI systems are not always fully transparent. Further, transparency in designing machine learning models can be achieved in creating additional awareness regarding transparency among the WP involved in the design and development of the AI system.

5) Diversity, non-discrimination and bias

The focus in HOLiFOOD should not only be on the typical grounds for discrimination as only very limited personal data is processed within the project, but also on possible new forms of discrimination (food

[35] Andreas Holzinger, Explainable AI (Ex-AI), Informatik-Spektrum, 2018.

hazards that may only stem from a certain area). All partners in HOLiFOOD must avoid unfair bias in any case. For diversity and non-discrimination D9.2 (Gender Audit) sets out that all partners are fully committed to integrate gender equality into all stages of the project. It is crucial to involve vulnerable groups and to grant access to the AI system without any form of discrimination.

6) Social and environmental well-being

The AI system shall have a positive impact on future generations as well as on the environment. Finding food hazards at an early stage seems to increase the well-being of humans, while reducing diseases. Read together with the following requirement a monitoring process is needed for the assessment of the actual positive impact, even though this assessment may be only possible after the AI component was developed. Contrary, it must also be considered that AI systems can consume a lot of energy. While describing the significant impact AI models can have on human rights from a legal perspective, it should be also noted here, that the application of trustworthy AI aims to be a safeguard for human dignity.

7) Accountability

This requirement means that potential risks for research participants as well as end-users must be evaluated before the development of the AI system and assessed afterwards, therefore records of processing activities must be made. The potential risk of data harm is considered low for HOLiFOOD, due to the fact that only limited personal data will be proceed in HOLiFOOD. Nevertheless it is essential, to ensure auditability measures to make it possible effectively identify problems. WP8 together with WP9 will reduce its potential risks by constant monitoring.

8.3 Ethics in Development of Platforms

Technical provisions, accessibility and governance practices of platforms have significant consequences for the level of human rights protection, both in terms of the opportunities they offer and the potential harm they can cause.[36] Platforms often allow a certain predefined kind of social engagement. As end-users are tempted not to consider the possible far-reaching consequences as long as only a few buttons have to be clicked[37], it is therefore HOLiFOOD's task to consider possible implications already during the development of the platform.

As previously stated, very limited personal data will be proceed on the HOLiFOODs platform. Despite this, by comparing different ethics guidelines for the use of personal data some key principles for the ethical use of personal data in HOLiFOOD must be considered:

1. **Lawfulness**: For all use of personal data there must be a legal basis as discussed in the legal section.
2. **Data subject protection:** Data subjects' rights, dignity, privacy and security have to be ensured and balanced against the positive outcomes of data use, where partners agreed on having a project-wide as far as possible approach of informed consent, which will be integrated in the platform together with the privacy policy created by WP8.
3. **Agency and informed consent:** The autonomy of the data subjects has to be respected and agency of data subjects should be promoted. WP8 created an informed consent template for the purposes of the project and the use of the collected data has to be based on informed consent as set out in the GA.[38] The Legal and Ethical Helpdesk can be approached for further adjustments, where necessary.
4. **Transparency and trustworthiness:** For the HOLiFOOD platform to achieve its aim, it must maintain the trust of researchers, stakeholders, and end-users. This should be encouraged through strong involvement of those stakeholders, and through transparency in the use of data.

8.4 Conclusion and Perspectives

The ambition for the project is to follow the highest ethical standards as described before and to establish a diverse, non-discriminatory environment to get the best result possible. HOLiFOOD,

[36] Rikke Frank Jørgensen, Human rights in the age of platforms, 2019, p.20
[37] Ibid.
[38] GA, Part B, p.40

especially WP8, aims to set up a new policy for ethical requirements striving from the upcoming legislation, such as AIA, DA and DGA, as an intersection for guidelines stemming from law, which are not engrained in law (yet). For this purpose, WP8 will set up, together with the coordination of WP9, an internal discussion session in spring 2024, to elaborate on the implementation of the ethical requirements and faced challenges.

9 Conclusion

In Deliverable 8.2 "Legal and Ethical Framework," a comprehensive overview of the legal and ethical considerations governing the development of technology and general conduct within the project has been provided. The primary aim of this report was to ensure adherence to relevant laws, regulations, and ethical standards.

This document serves as a foundational guide for project partners, the project as a whole, and the coordination team to navigate the landscape of legal and ethical requirements. This ongoing commitment to legal and ethical compliance ensures that HOLiFOOD remains at the forefront of responsible and innovative research in the food technology domain.

The dissemination of D8.2 and its content will be a strategic and inclusive process, reaching both internal consortium members and external stakeholders. Within the consortium, presentations and discussion sessions tailored to the specific needs and interests of consortium members are offered by the legal and ethical partner UNIVIE. Furthermore, UNIVIE will also provide written guidelines dealing with legal issues within the HOLiFOOD project. These documents will be sent via the legal and ethical helpdesk to the consortium and or to the partners concerned, depening on the specific topic. Regular face to face meetings and conference calls will facilitate ongoing dialogue, allowing for the exchange of ideas and feedback to further refine our approach to legal and ethical compliance. Externally, HOLiFOOD is committed to sharing its findings with a broader audience. To achieve this, the project will leverage various channels and platforms. All public deliverables, including D8.2, will be disseminated through the project website, ensuring transparency and accessibility. Additionally, key findings and insights will be presented at relevant conferences, seminars, and workshops to engage with the wider research community and stakeholders in the field of food safety and sustainability.

10 Annex A: Joint Controllership Arrangement

1. Context

All data protection terms, if not otherwise stated in this Arrangement, shall be understood in the sense of the GDPR.

Joint Controllers set jointly the purpose and means of the processing (Article 26 GDPR). This requires an Arrangement pursuant to Article 26 GDPR. Therefore, this present Arrangement addresses the following topics:

- The subject matter of data processing,
- The nature and the purpose of the processing,
- The type of personal data and categories of data subjects and
- The obligations and rights of the Joint Controllers.
- The engagement of Data Processors.

Each Controller is represented by a PI as described in Point 2.2 of the Informed Consent. This Arrangement shall enter into force at the date of the agreement and confirmation of each party by its contact point outlined in 2.2 via e-mail. All amendments to this Arrangement may also be concluded electronically via e-mail.

2. Joint Controllers

Acronym	Institution	Country	Contact Point	Contact Details
WR	STICHTING WAGENINGEN RESEARCH	NL	Ine van der Fels-Klerx	ine.vanderfels@wur.nl
AGROKNOW	AGROKNOW IKE	EL	Marilena Dimitrakopulou	marilena.dimitrakopoulou@agroknow.com
APRE	AGENZIA PER LA PROMOZIONE DELLA RICERCA EUROPEA	IT	Sara Gentilini	gentilini@apre.it and gdpr@apre.it
CREME	CREME SOFTWARE LTD	IE	William O'Sullivan	holifood@cremeglobal.com
DIA	DIALOGIK GEMEINNUTZIGE GESELLSCHAFT FUR KOMMUNIKATIONS UND KOOPERATIONSFORSCHUNG MBH	DE	Ludger Benighaus	lbenighaus@dialogik-expert.de

EUFIC	EUROPEAN FOOD INFORMATION COUNCIL	BE	Maria Scherbov	maria.scherbov@eufic.org
UVMB	ALLATORVOSTUDOMANYI EGYETEM	HU	Ákos Józwiak	jozwiak.akos@univet.hu
INRAE	INSTITUT NATIONAL DE RECHERCHE POUR L'AGRICULTURE, L'ALIMENTATION ET L'ENVIRONNEMENT	FR	Jeanne-Marie Membré	jeanne-marie.membre@inrae.fr
CNR	CONSIGLIO NAZIONALE DELLE RICERCHE	IT	Vincenzina Fusco	vincenzina.fusco@ispa.cnr.it
UNEW	UNIVERSITY OF NEWCASTLE UPON TYNE	UK	Lynn Frewer	Lynn.Frewer@newcastle.ac.uk

Table: Joint Controllers involving Stakeholders in the HOLiFOOD project

3. Data Subjects

Data Subjects will be the stakeholders (natural persons) representing actors (legal entities) operating in the food safety risk sector (e.g.research, laboratories, FS services, consumers' associations, industry and farmers associations, communicators), who participate in the HOLiFOOD project.

4. Data Processor(s)

The Joint Controllers jointly decided to use Microsoft Teams to store data subjects' data. In case of a change of the Data Processor, all Joint Controllers need to agree to the selection of the new Data Processor.

Microsoft acts as Data Processor and is governed by the following data processing agreement (DPA): https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

To achieve the purpose(s), Data Controllers may use further Data Processors. A Processor is a natural or legal person, public authority or other body, which processes personal data on behalf of the Controller (Article 4(8) GDPR). Each Joint Controller remains responsible to ensure compliance with EU Regulations as well as national law and inform other Joint Controllers and Data Subjects accordingly.

5. Point of Contact for the Data Subjects

Stichting Wageningen Research (WR) is the main point of contact for the data subjects. WR will also keep the joint repository (Microsoft Teams) updated and is responsible to ensure data subject rights.

Ine van der Fels-Klerx	ine.vanderfels@wur.nl
Nathan Meijer	nathan.meijer@wur.nl

WR shall inform all Joint Controllers without a due delay in case of an exercise of Data Subjects' rights.

Furthermore, Data Subjects' will be provided with all contact details of each Joint Controller to exercise also their rights directly at each institution.

6. Purpose(s) of Processing Activities

The overall objective of HOLiFOOD is to improve the integrated food safety risk analysis framework in Europe to:

a) Meet future challenges arising from Green Deal policy driven transitions in particular in relation to climate driven changes,
b) Contribute to the UN's Sustainable Development Goals and
c) Support the realisation of a truly secure and sustainable food production.

In order to align with stakeholder priorities, preferences and user requirements, the HOLiFOOD innovations will be designed and tested through a multi actor approach involving stakeholders. Several online and offline workshops, interviews and consultations will be organised, where external stakeholders will be invited.

The overarching purpose for the processing of the personal data of external Stakeholders is scientific research in the field of food safety risk analysis in particular for the HOLiFOOD project.

Data	Purpose(s) of Processing
Stakeholders' - name(s) - e-mail address(es) - affiliation(s) - video and audio recording(s)	- Communication and execution of the workshops, interviews and consultations (including follow-ups after the workshop). - Analysing stakeholders' preferences and perspectives - Review of the HOLiFOOD project by the Commission

Table: Category of Personal Data Processed and Purposes of Processing Activities

Joint Controllers may only process Stakeholders' data for the purpose outlined in the table above.

7. Legal Basis for Processing Personal Data

The legal basis for processing Stakeholders' personal data is informed consent in accordance with Article 6(1) (a) GDPR. Each Joint Controller who contacts Stakeholders for the first time makes sure that the data subject is provided with all necessary information and an informed consent is given. Each Joint Controller shall use the informed consent form provided on the HOLiFOOD website to obtain consent from the Stakeholder.

8. Data Storage and Security

Stakeholders' Data will be stored on the Stichting Wageningen Research Repository (project coordinator) using Microsoft Teams until the end of the HOLiFOOD project including the period of the review of the project by the Commission. Stichting Wageningen Research (WR) controls and monitors the access to the personal data. Only Joint Controllers shall have access to the personal data.

Microsoft secures all personal data through technical and organisational measures to ensure that it is protected from unauthorised access, alteration, or loss.
Core elements are:

- Azure Active Directory (Azure AD), which provides a single trusted back-end repository for user accounts. User profile information is stored in Azure AD through the actions of Microsoft Graph.
- There may be multiple tokens issued which you may see if tracing your network traffic, including Skype tokens you might see in traces while looking at chat and audio traffic.
- Transport Layer Security (TLS) encrypts the channel in motion. Authentication takes place using either mutual TLS (MTLS), based on certificates, or using Service-to-Service authentication based on Azure AD.
- Point-to-point audio, video, and application sharing streams are encrypted and integrity checked using Secure Real-Time Transport Protocol (SRTP).
- You will see OAuth traffic in your trace, particularly around token exchanges and negotiating permissions while switching between tabs in Teams, for example to move from Posts to Files. For an example of the OAuth flow for tabs, see this document.
- Teams uses industry-standard protocols for user authentication, wherever possible.

More information may be found in the security guide: https://learn.microsoft.com/en-gb/microsoftteams/teams-security-guide

Each Data Controller may also store the personal data on local repositories. Each Data Controller must ensure that technical and organisational measures are in place to ensure unauthorised access, alteration, or loss.

9. Data Breach Notification

Joint Controllers must inform each other immediately and completely if errors or irregularities in data processing are discovered.

Each Joint Controller shall inform the other Joint Controllers in writing and without undue delay, and no later than 24 hours having become aware of it, of any violation of the protection of personal data within the meaning of Article 4(12) of the GDPR ("personal data breach").

Microsoft acts as Data Processor. If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident. For more information: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

10. Sharing of Data with Third Parties

Each Joint Controller shall ensure that personal data of Stakeholders is not included in the deliverables. Data may be shared with Data Processors in order to achieve the purpose outlined in point 2.5.

11. Transfer of Data to Third Country

One of the Joint Controllers is based in the UK. The transfer of personal data from the European Union to the United Kingdom as an agreement refers to the adequacy decision rendered by the European Commission (Commission Implementing Decision of 28.6.2021, C(2021) 4800 final). With regard to the transfer of personal data from the United Kingdom to the European Union, this agreement refers to the adequacy regulations established in the United Kingdom.[39]

With respect to the use of Microsoft Teams all transfer of personal data out of the European Union is governed by the 2021 Standard Contractual Clauses implemented by Microsoft and Article 46 of the GDPR. Article 46(1) of the GDPR permits the transfer

[39] See United Kingdom Department for Digital, Culture, Media and Sport, 'International data transfers: building trust, delivering growth and firing up innovation' (26 August 2021) <https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation>; see also Information Commissioner's Office, 'International transfers after the UK exit from the EU Implementation Period', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/.

of personal data to a third country or an international organisation if appropriate safeguards are provided and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided by standard data protection clauses adopted by the European Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR.

The 2021 Standard Contractual Clauses (P2P) is a Data Transfer Agreement between Microsoft Irelands Operations Limited within the EU and Microsoft Corporation in the US. These standard data protection clauses were adopted by the European Commission in June 2021 and implemented by Microsoft in September 2021. The clauses govern the transfer of personal data from the EU to the US, the implementation of appropriate data protection safeguards (clause 8), the enforceability of data subject's rights (clause 10) and effective legal remedies (clause 11).

In accordance with its Products and Services Data Protection Addendum (DPA) of January 2023, Microsoft will abide by the requirements of European Economic Area and United Kingdom, data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and Clause 8 of the 2021 Standard Contractual Clauses. Such transfers and safeguards will be documented according to Article 30(2) of the GDPR and Clause 8.9 of the 2021 Standard Contractual Clauses.

For more information on Microsoft compliance with EU transfer requirements for personal data in the Microsoft Cloud - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRql1.

11 Annex B: Informed Consent Template

1. Context

Informed consent is an essential building block of research ethics. In order to participate in an EU funded project it is therefore required to seek for an informed consent. Furthermore, we intend to process your personal data only based on your consent (in accordance with Article 6(1)(a) GDPR).

Consequently, this document infoms you about your participation in the EU funded research project as well as the processing of your personal data, which is required for the project. Only after you consented to all of the below, we will involve you in the project and process your personal data.

Additionally, we ask you not to share or further process any of the personal data or business sensitive information disclosed to you with any third party (i.e., with any individual or entity that is not a participant to the call).

2. Your Involvement in the HOLiFOOD Project

The overall objective of HOLiFOOD is to improve the integrated food safety risk analysis framework in Europe to:

a) Meet future challenges arising from Green Deal policy driven transitions in particular in relation to climate driven changes,
b) Contribute to the UN's Sustainable Development Goals and
c) Support the realisation of a truly secure and sustainable food production.

In order to align with stakeholder priorities, preferences and user requirements, the HOLiFOOD innvovations will be designed and tested through a multi actor approach involving stakeholders. Several online and offline workshops, interviews and consultations will be organised, where external stakeholders like you will be invited.

2.1 Your Participation

Your involvement is voluntary and you can discontinue your involvement in the research at any time.

2.2 Your Main Contact point

Stichting Wageningen Research (WR) – HOLiFOOD Project Coordinator

Ine van der Fels-Klerx	ine.vanderfels@wur.nl
Nathan Meijer	nathan.meijer@wur.nl

3. Processing Your Personal Data

3.1 Contact Details of the Joint Controllers

Several partners of the HOLiFOOD project concluded a Joint Controllership Arrangement pursuant to Article 26 GDPR outlining the rights and obligations of the Joint Controllers. The essence of the arrangement is made available to you via this document. If you have any specific questions, please feel free to contact any of the Joint Controllers:

Akronym	Institution	Country	Contact Point	Contact Details
WR	STICHTING WAGENINGEN RESEARCH	NL	Ine van der Fels-Klerx	ine.vanderfels@wur.nl
AGROKNOW	AGROKNOW IKE	EL	Marilena Dimitrakopulou	marilena.dimitrakopoulou@agroknow.com
APRE	AGENZIA PER LA PROMOZIONE DELLA RICERCA EUROPEA	IT	Sara Gentilini	gdpr@apre.it
CREME	CREME SOFTWARE LTD	IE	William O'Sullivan	holifood@cremeglobal.com
DIA	DIALOGIK GEMEINNUTZIGE GESELLSCHAFT FUR KOMMUNIKATIONS UND KOOPERATIONSFORSCHUNG MBH	DE	Ludger Benighaus	lbenighaus@dialogik-expert.de
EUFIC	EUROPEAN FOOD INFORMATION COUNCIL	BE	Maria Scherbov	maria.scherbov@eufic.org
UVMB	ALLATORVOSTUDOMANYI EGYETEM	HU	Ákos Józwiak	jozwiak.akos@univet.hu
INRAE	INSTITUT NATIONAL DE RECHERCHE POUR L'AGRICULTURE, L'ALIMENTATION ET L'ENVIRONNEMENT	FR	Jeanne-Marie Membré	jeanne-marie.membre@inrae.fr
CNR	CONSIGLIO NAZIONALE DELLE RICERCHE	IT	Vincenzina Fusco	vincenzina.fusco@ispa.cnr.it
UNEW	UNIVERSITY OF NEWCASTLE UPON TYNE	UK	Lynn Frewer	Lynn.Frewer@newcastle.ac.uk

Table: Joint Controllers involving Stakeholders in the HOLiFOOD project

If you want to exercise your data subject rights or have questions regarding your involvement in the project, please contact the project coordinator (your main contact point):

Ine van der Fels-Klerx	ine.vanderfels@wur.nl
Nathan Meijer	nathan.meijer@wur.nl

Stichting Wageningen Research (WR), the project coordinator, will also keep the joint repository (Microsoft Teams) updated and is responsible to ensure your rights. You can also contact each Joint Controller directly.

3.2 Category of Personal Data and Purpose of the Processing

Data	Purpose(s) of Processing
Stakeholders' - Name(s) - e-mail address(es) - affiliation(s) - video and audiorecording(s)	- Communication and execution of the workshops, interviews and conusltions (including follow-ups after the workshop). - Analysing stakeholders' preferences and perspectives - Review of the HOLiFOOD project by the Commission

Table: Category of Personal Data Processed and Purposes of Processing Activities

The overarching purpose of the processing your personal data is scientific research in the field of food safety risk analysis, in particular for the HOLiFOOD project.
Information gathered from your involvement will be also anonymised and used in project activities, such as publications, conferences, disseminations on the project website and social media channels. In case we would like to name you in a deliverable or scientific publication, you will be contacted for this purpose seperatly again.

3.3 Legal Basis

The legal basis for processing your personal data is informed consent in accordance with Artcle 6(1)(a) GDPR.

3.4 Recipients of the Personal Data/Sharing of your Data with Third Parties

Microsoft acts as Data Processor and is governed by the following data processing agreement (DPA): https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

Data may be shared with Data Processors in order to achieve the purpose. In this case we will inform you separately about the Data Processor.

3.5 Transfer of Data to Third Countries

One of the Joint Controllers is based in the UK. Your data will therefore be transferred there. The transfer is based on the adequacy decision issued for the United Kingdom by the European Commission in accordance with Art. 45 of the GDPR.[40]

With respect to the use of Microsoft Teams all transfer of personal data out of the European Union is governed by the 2021 Standard Contractual Clauses implemented by Microsoft and Article 46 of the GDPR.

3.6 Period of Data Storage

Your Data will be stored on the Stichting Wageningen Research Repository (project coordinator) using Microsoft Teams until the end of the HOLiFOOD project including the period of the review of the project by the Commission. All data is stored within the EU. Stichting Wageningen Research (WR) controlls the access to the personal data. Joint Controllers will process and store your personal data only for the purposes outlined above.

3.7 Data Security

Microsoft secures all personal data through technical and organisational measures to ensure that it is protected from unauthorised access, alteration, or loss.
Core elements are:

- Azure Active Directory (Azure AD), which provides a single trusted back-end repository for user accounts. User profile information is stored in Azure AD through the actions of Microsoft Graph.
- There may be multiple tokens issued which you may see if tracing your network traffic, including Skype tokens you might see in traces while looking at chat and audio traffic.
- Transport Layer Security (TLS) encrypts the channel in motion. Authentication takes place using either mutual TLS (MTLS), based on certificates, or using Service-to-Service authentication based on Azure AD.
- Point-to-point audio, video, and application sharing streams are encrypted and integrity checked using Secure Real-Time Transport Protocol (SRTP).
- You will see OAuth traffic in your trace, particularly around token exchanges and negotiating permissions while switching between tabs in Teams, for example to move from Posts to Files. For an example of the OAuth flow for tabs, see this document.
- Teams uses industry-standard protocols for user authentication, wherever possible.

[40] See United Kingdom Department for Digital, Culture, Media and Sport, 'International data transfers: building trust, delivering growth and firing up innovation' (26 August 2021) <https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation>; see also Information Commissioner's Office, 'International transfers after the UK exit from the EU Implementation Period', https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/.

More information may be found in the security guide: https://learn.microsoft.com/en-gb/microsoftteams/teams-security-guide.

Each Data Controller may also store the personal data on local repositories. Each Data Controller ensures that technical and organisational measures are in place to ensure unauthorised access, alteration, or loss.

3.8 Your Rights under GDPR

The General Data Protection Regulation (GDPR) grants you the following rights:

The right to be informed	This means we must inform you of how we are going to use your personal data. We do this through this form and by informing you of how your data will be used each time we collect it (Article 13).
The right of access	You have the right to access your personal data that we store. To request access to your data, please email the Data Controllers identified above. We will respond to your request within one month (Article 15).
The right to rectification	If you think the data we store about you is incorrect, please let us know so we can correct it. You can do this by emailing the Data Controllers identified above (Article 16).
The right to erasure	You have the right to request that we delete your data and we will do so. You can do this by emailing the Data Controllers identified above (Article 17).
The right to restrict processing:	Article 18 of the GDPR gives you the right to obtain from any Data Controller restriction of processing in certain contexts (Article 18).

The right to data portability	You have the right to receive the personal data concerning you, which you have provided to the Data Controller(s) in a structured, commonly used and machine-readable format, and have the right to transmit those data to another controller without hinderance from the controller to which the personal data have been provided pursuant to Article 20 of the GDPR.
The right not to be subject to a decision based solely on automated processing	There will be no automated decision-making and profiling (Article 22).
The right to withdraw consent at any time	If you withdraw your consent, Joint Controllers will no further process your data. However, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Article 7).
The right to lodge a complaint with a supervisory authority	If you are a data subject in the EU, please find the supervisory authority of your country here.

4. Your Consent

I have read this form and fully understand the contents of it.

Please check the initial box after each statement.

Ethical Consent:

I understand and I consent that I will be part of the EU funded research project HOLiFOOD (Projectnumber: 101059813).	

Data Proctection Law Consent:

I understand and I consent that I give the Joint Controllers permission to process my personal data for the purposes outlined in this form.	

Non-Disclosure Agreement:

I hereby declare that I will not record, process nor share personal data or business sensitive information disclosed to me with any third party (i.e., with any individual or entity that is not a participant to the call).	

Yes, I want to participate in HOLiFOOD project and confirm my consents given above.	No, I do not want to participate

holi food

Funded by
the European Union