ALLIANCE

A hoListic framework in the quality Labelled food supply chain systems' management towards enhanced data Integrity and verAcity, interoperability, traNsparenCy, and tracEability

D1.2 - INITIAL DATA MANAGEMENT PLAN, ETHICS, FUNDAMENTAL RIGHTS, DATA AND PRIVACY ISSUES

GRANT AGREEMENT NUMBER: 101084188

This project has received funding from the European Union's HE research and innovation programme under grant agreement No 101084188

Lead Beneficiary: **WISE4**

Type of Deliverable: DMP - Data Management Plan

Dissemination Level: Public

Submission Date: 28.04.2023

Version: 2.0

Versioning and contribution history

Version	Description	Contributions
0.1	The initial draft of the deliverable	WISE4
1.0	The reviewed draft of the deliverable	UTH
1.1	The final draft of the deliverable	WISE4
2.0	The final draft to be submitted	UTH

Authors

Author	Partner
Maria Kadena	WISE4

Reviewers

Name	Organisation
Apostolos Apostolaras	UTH
Stavroula Maglavera	UTH

Disclaimer

The information and views set out in this publication are those of the author(s) and do not necessarily reflect the official opinion of the European Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use, which may be made of the information contained therein.

Table of contents

1 Introduction 6
2 Data Summary 7
2.1 Data Collection and Generation in ALLIANCE 7
2.2 Data types and sources 8
2.3 Data formats and size 8
2.4 Data repositories 9
2.5 Guiding principles for data collection, storage and quality assurance 9
3 FAIR Data Management 12
3.1 Making data findable, including provisions for metadata 12
3.2 Making data openly accessible 12
3.3 Making data interoperable 12
3.4 Increase data re- use (through clarifying licences) 13
4 Allocation of resources 14
5 Data Privacy and Ethics in Food Technology and Blockchain 15
6 Data security 17
7 Legal and Ethical Aspects 19
7.1 ALLIANCE's Compliance 20
8 Fundamental Rights Consideration 22
Appendix 1 25
Appendix 2 28
Appendix 3 31

List of figures

Figure 1 ALLIANCE Architecture..... 8
Figure 2 – ALLIANCE OneDrive (shared folder) 17

List of Abbreviations

Abbreviation	Description
AI	Artificial Intelligence
ALLIANCE	A holistic framework in the quality Labelled food supply chain systems' management towards enhanced data Integrity and veracity, interoperability, transparency, and traceability (Project Acronym)
CC BY	Creative Commons Attribution
DMP	Data Management Plan
DOI	Digital Object Identifier
DPO	Data Protection Officer
EC	European Commission
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
FSC	Food Supply Chain
GDPR	General Data Protection Regulation
GI	Geographical Indication
ICT	Information and Communication Technology
IoT	Internet of Things
IPR	Intellectual Property Rights
OA	Open Access
PDO	Protected Designation of Origin
PGI	Protected Geographical Indication
PI	Principal Investigator
URL	Uniform Resource Locator
UTH	University of Thessaly

Executive Summary

Deliverable D1.2 presents the Initial version of the ALLIANCE Data Management Plan, which is delivered on M6 of the project. The DMP is a living document during the whole lifetime of the ALLIANCE. The deliverable outlines how the data will be collected, produced and used within ALLIANCE. It also describes how these data will be shared, will be made accessible for re-use and further exploitation, and how they will be curated, preserved or deleted when necessary. ALLIANCE has made sure to comply with GDPR and national regulations, while also following the FAIR principles, in order to handle the data in a legal and ethical manner.

This document follows the template provided by the European Commission in the Horizon Europe Participant Portal.

As this is an initial version of the ALLIANCE Data Management Plan presented in month M6 of the project, the data described at this early stage, are a preliminary reflection of the data that we foresee to be used and collected. We anticipate that during the evolution of the project, there will be certain changes either to the content of the datasets or the information classification.

Monitoring the status of the data on a regular basis will ensure that the DMP is implemented as planned. It is noted, however, that, even though certain updates will be introduced as the project and the development of its solutions evolves, the main principles as described within this deliverable, are anticipated to remain intact until the end of the project. These principles the main strategic axes of the overall Data Management Plan.

The DMP serves a dual purpose. First, it acts as a guide for project partners on the appropriate collection, handling, curation, and preservation of data in compliance with the GDPR and the project's ethics strategy. Second, the DMP provides external parties interested in ALLIANCE with information about the data collected and generated within the project, including access and potential reuse. To do so, the DMP outlines how data is processed, curated, and stored for those collaborating with ALLIANCE on the multi-actor platforms of the seven Demonstrators that serve as the foundation for the research and innovation of the project.

1 Introduction

In ALLIANCE, the data management plan is a document that describes the data collected and generated by the project, the procedures used by the project to curate data, and how the project is fostering the adoption of the FAIR principles by ensuring that rules are defined to improve data findability, accessibility, interoperability, and reusability. The data management plan (DMP) allows to identify of risks for the future sharing and reusing of the data collected and produced during the ALLIANCE activities, and thus to define ways to solve corresponding issues or to mitigate these risks as early as possible.

Here, it is important to note how we understand research data. Research data can be defined as any information that has been collected, observed, or created for scientific purposes. This type of data normally includes statistics, results of experiments and simulations, measurements, observations resulting from fieldwork or remote sensing techniques, survey results, interview recordings, and images. In the context of this document, we focus mainly on data in digital form, even if non- digital formats such as laboratory notebooks and diaries are usually part of this category.

This deliverable is part of Work Package 1 (WP1) of ALLIANCE, which focuses on data management and sharing across different disciplines and domains. Specifically, it contributes to Task 1.5, which aims to establish a common approach for data management and metadata creation. As such, this deliverable provides detailed guidance on how to ensure data quality and findability, and how to handle data in a legally and ethically compliant manner. By following the guidelines set out in this deliverable, project partners will be able to ensure that their data conforms to the FAIR principles and meets GDPR and national regulations. Overall, this deliverable is an important component of ALLIANCE's efforts to create a seamless and interoperable data-sharing infrastructure across different domains and disciplines.

The document is structured as follows:

- Chapter 2 - Data Summary: description of the purpose and use of data within ALLIANCE, data handling and storage procedures and Data Privacy Issues.
- Chapter 3 - FAIR Data Management: description of how ALLIANCE will implement the FAIR (Findable, Accessible Interoperable, and Re- usable) principles
- Chapter 4 - Allocation of resources: description of associated costs and personnel
- Chapter 5 - Data security: how the security of data will be ensured
- Chapter 6 - Ethical aspects: how personal and sensitive information will be duly protected
- Appendix 1- Template Consent Form
- Appendix 2 - ALLIANCE Research Agreement
- Appendix 3 – Data types, size, sources and management per Partner

2 Data Summary

2.1 Data Collection and Generation in ALLIANCE

The main concept of ALLIANCE is the introduction of a paradigm shift in the management of Food Supply Chain (FSC) Systems for the combat against Food Fraud, distinguishing from the traditional approaches that leverage digitalized logistic solutions and standalone FSC interoperability protocols. ALLIANCE aims to provide a holistic framework that safeguards data integrity and veracity, enhances traceability and transparency and reinforces interoperability in quality labelled supply chain of organic, PDO (Protected Designation of Origin), PGI (Protected Geographical Indication), and GI (Geographical Indication) food, through innovative technology solutions and validated approaches (such as use of in-situ portable rapid testing devices to detect adulteration and verify food origin and authenticity) and fosters evidence-based decision making through AI and ML for preventative interventions and actionable planning. [1]

The data collection and generation in ALLIANCE will be performed through various sources, including IoT devices, sensors, blockchain technology, and AI-based tools. These sources will work together to provide accurate, timely, and secure data related to the quality-labelled food supply chain. In particular, **IoT devices and sensors** will be used to collect **real-time data** related to food production, processing, and transportation. This data will be **stored in the ALLIANCE blockchain platform** to ensure its authenticity, traceability, and transparency.

AI-based tools will be used to analyse this data and identify patterns, trends, and potential risks related to food fraud. The Vulnerability Risk Assessment Management Framework (Task 2.3) will use AI to analyse data and measurements related to various parameters, such as the performance of operational and production procedures, commodity supply/demand fluctuations, environmental factors, and market trends and price variability. This analysis will help to proactively identify and control vulnerabilities in quality-labelled food production, processing, and transportation that can lead to food fraud and raise safety risks.

The Delphi technique will be used to gather input from experts regarding the performance of existing solutions, the improvement of identified gaps, essential needs, and discrepancies identified. This technique involves a structured communication process where experts provide their opinions and feedback on a specific topic. The results of this technique will help to identify food actors and points in the food supply chain that demonstrate low performance, lack or low levels of trust, and are characterized by high risk of fraudulent activities.

ALLIANCE, involves carrying out data collection, including personal data and metadata (in the context of validation campaigns and the consumer surveys). All processing of personal data will be conducted in accordance with the provisions of: a) the GDPR (Regulation (EU) 2016/679), b) the Universal Declaration of Human Rights and the Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, and c) the national laws applying its provisions, including those governing the acquisition of valid consent.

Personal data managed during ALLIANCE will be processed only under one of the following legal bases: (i) When the data subject has given her/his consent; (ii) When the processing is necessary for the performance of or the entering into a contract; (iii) When processing is necessary for compliance with a legal obligation; (iv) When processing is necessary in order to protect the vital interests of the data subject.

1 https://ec.europa.eu/research/participants/documents/download?documentIds=080166e5e8de6938:PROPOSAL_101084188-ALLIANCE-HORIZON-CL6-2022-FARM2FORK-01&appId=PPGMS&rendition=true

Overall, the data collection and generation in ALLIANCE will be based on advanced technologies that work together to ensure the authenticity, traceability, and transparency of the quality-labelled food supply chain while proactively identifying and controlling vulnerabilities that can lead to food fraud and safety risks.

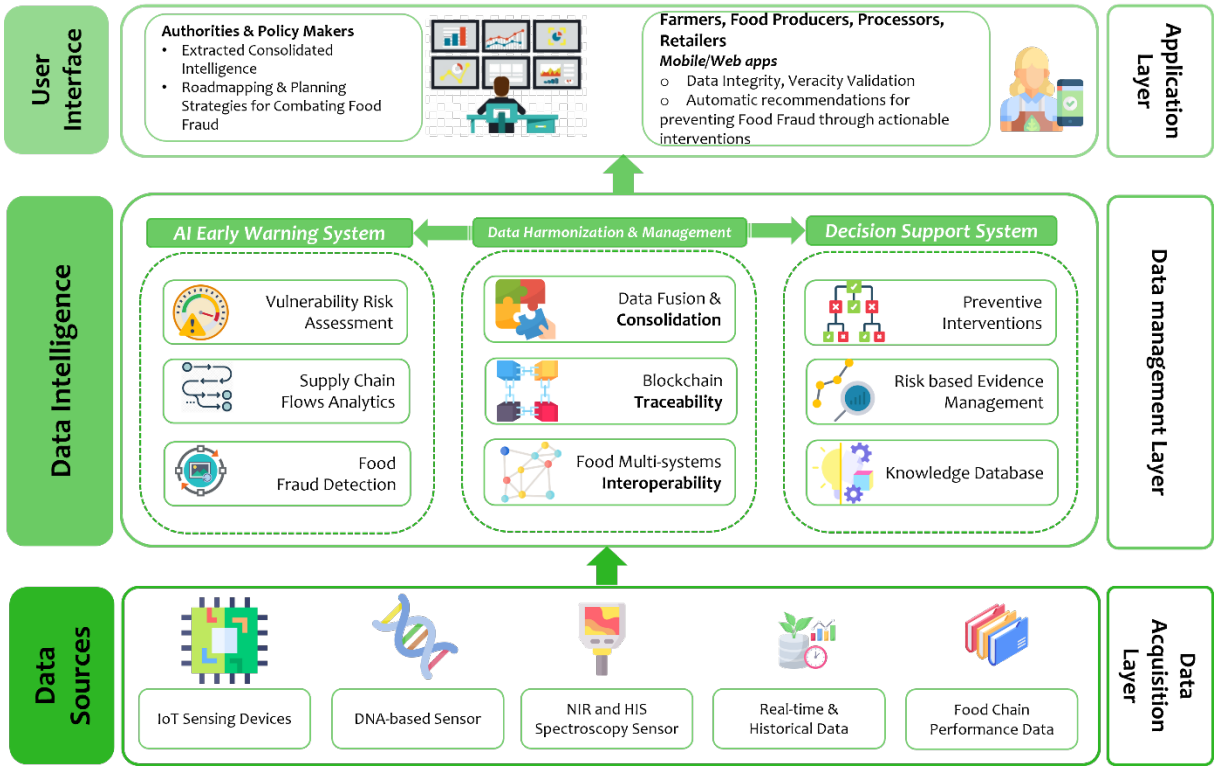

Figure 1 ALLIANCE Architecture[2]

2.2 Data types and sources

The sources of data collection will include various stakeholders involved in the FSCs, such as suppliers, manufacturers, retailers, and consumers. The data will be collected through surveys, questionnaires, interviews, focus groups, and other forms of market research. IoT devices and sensors will be installed in the supply chain to collect performance monitoring data. Other data sources may include social media, news articles, and other publicly available sources of information.

ALLIANCE is expected to generate and collect various types of data from different sources. It has been noted that some partners may not have a complete understanding of the types of data they collect or the sources from which they obtain it, as the project is still in its early stages. However, based on the information provided by several partners, the types of data and their respective sources are documented in detail in APPENDIX 3.

2.3 Data formats and size

ALLIANCE will generate and use data in various formats, such as numerical data, texts, images, tables, and other formats. The size of the data will depend on the specific data type and the volume of data generated during the project. As ALLIANCE involves the use of IoT devices, the generated data could potentially be quite large. At the time of writing this initial version of the

2 ALLIANCE | D1.1 - Project Management Handbook

DMP, the size of datasets is not fully clear. However, based on the information provided by several partners, the formats of data and their size are documented in detail in APPENDIX 3. Additional information will be added in updates of this DMP as this becomes available.

2.4 Data repositories

In ALLIANCE, the shared data will be deposited in an Open data repository that will be identified through the platform of re3data [3]. The project will use trusted repositories such as Zenodo[4], DRYAD[5], and Harvard Dataverse[6] for general data, among others. The deposited data will have persistent identifiers (PIDs) such as Digital Object Identifiers (DOIs) and will be well-documented with clear license and provenance information. The data will be archived and stored in a secured and encrypted form using strong cryptographic protocols in servers indicated by the pilots or technology providers, and agreed upon within the consortium. The exact data repositories used have not been identified at the time this deliverable is written and may be subject to change as the project progresses. However, based on the information provided by several partners, the repositories are documented in detail in APPENDIX 3

However, the Data Management Plan (DMP) for ALLIANCE aims to ensure that the data is stored and managed efficiently, and in accordance with the related soft law instruments governing scientific research, such as the European Code of Conduct for Research Integrity, the Guidelines to rules on Open Access to Scientific Publications & Open Access to Research Data in Horizon Europe, and the Guidelines on Data Management in Horizon Europe. Additionally, the DMP emphasizes the use of open data standards and the use of community-agreed schemas, controlled vocabularies, keywords, thesauri or ontologies where possible in order to ensure interoperability and integration with other data, applications, and workflows.

2.5 Guiding principles for data collection, storage and quality assurance

i) Principles for collecting and processing of open data

Data collected and processed to support research and innovation actions in ALLIANCE can be uploaded to the ALLIANCE OneDrive repository with appropriate metadata and attribution (stored in UTH premises server which is located within EU), and made openly accessible to the consortium under the "Project Data (Open Access)" folder. External parties can request access to these data, having limited or full editing or viewing rights, through a link. External sharing Is possible with. However, if processed data is intended for use in products that may have intellectual property, copyright, or patent implications, then it may be stored in the "Project Data (Restricted Access)" folder, which is not shared or published before the end of the project.

ii) Principles for collecting and processing restricted access data

The collection of data with restricted access, including proprietary information, requires the establishment of a data-sharing agreement with the provider. The agreement should detail how the data will be accessed, shared, and processed, and any applicable restrictions or licenses.

3 https://www.re3data.org/

4 A data and publication repository, developed by CERN in the OpenAIRE project, freely available to all research programs. (https://zenodo.org/)

5 https://datadryad.org/stash

6 https://dataverse.harvard.edu/

To store the restricted access data, they should be uploaded to the ALLIANCE OneDrive repository with appropriate metadata and attribution, and stored in folders created specifically for this purpose within the Project Data (Restricted Access) folder. Access to this folder will be managed by the repository manager and can be granted or denied to specified individuals or user groups within the project.

Restricted access to data copies can only be held locally using the OneDrive synchronization and data access protocols. All copies outside this secure environment must be deleted.

iii) Principles for collecting and processing of personal data and data reflecting traditional and local knowledge

The following procedures are established for the collection and storage of personal data:

- ⇨ A clear description of the scope and purpose of the data collection activity must be documented, including the procedures and criteria for identifying and recruiting participants.
- ⇨ A documented procedure for gaining explicit consent from participants must be established, including the provision that participation is restricted to adults and is voluntary. These procedures can be established using templates of informed consent/assent forms and information sheets available in the Project Resources section of the ALLIANCE OneDrive.
- ⇨ For data collected outside the European Union, explicit confirmation must be obtained from the mandated authorities that the data can be transferred in compliance with national laws and subjected to any processing required. This confirmation must be documented and stored in the respective access-restricted folder.
- ⇨ Personal data stored within the access-restricted sections of the ALLIANCE OneDrive must remain confidential and access granted only to designated individuals or partners in the project. Data must be irreversibly anonymized before being made public and stored in any part of the repository that is accessible by all beneficiaries and possibly shared with third parties, or uploaded to Zenodo, DRYAD, and Harvard Dataverse as a published and publicly accessible dataset.
- ⇨ Copies of personal data can only be held on the local drives using the OneDrive synchronization and data access protocols. All copies outside this secure environment should be deleted.

iv) Data Quality Assurance

The Quality Assurance process for data collected and generated by ALLIANCE will include the following steps:

For collected data:

- Raw datasets will be stored in a dedicated folder in the ALLIANCE OneDrive repository.
- Data will be checked and edited for quality, completeness, consistency, and accuracy by the responsible ALLIANCE partner.
- Metadata will be compiled, including both generic and domain-specific information, reporting a brief summary of the editing process.
- The final version of the datasets will be stored in a dedicated folder in the ALLIANCE OneDrive repository.
- If relevant for maintenance after the project lifetime, the final version of the datasets will also be uploaded to the Zenodo, DRYAD, and Harvard Dataverse repository.

For generated data:

- Metadata will be compiled, including both generic and domain-specific information, reporting a brief summary of the generation process (lineage).
- The final version of all generated datasets will be stored in a dedicated folder in the ALLIANCE OneDrive repository.
- If relevant for maintenance after the project lifetime, the final version of selected datasets will also be uploaded to the Zenodo, DRYAD, and Harvard Dataverse repository.

v) Legal Framework

The personal data collected, processed, and published by ALLIANCE adhere to the General Data Protection Regulation[7] (GDPR), which applies to all member states of the EU, including Greece, where UTH is legally based as the lead beneficiary of the project. ALLIANCE follows GDPR procedures as a minimum requirement and adheres to national/regional regulations and local customs and values. In cases where the legal stipulations of countries outside the EU are stricter, ALLIANCE applies the stricter definition. The GDPR provides specific rights to individuals whose personal data is processed in the project. These rights include the ability to obtain information on personal data processing, access personal data, request incorrect or incomplete data to be corrected, deleted or restricted, and to contest decisions based on automated processing. These rights can be exercised by any participant in the research at any time through the Coordinator, whose contact details are provided in the consent agreement.

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC https://eur-lex.europa.eu/eli/reg/2016/679/oj

3 FAIR Data Management

ALLIANCE follows the FAIR Data Management Principles recommended by the European Commission to ensure that the data produced by the project is easily accessible and reusable by the research community. The availability and use of the data depend on whether it is public or confidential and the specific license that applies to each dataset. As described in Chapter 2, ALLIANCE has established procedures to manage confidential data and protect the privacy of participants in the data collection activities conducted by the project.

3.1 Making data findable, including provisions for metadata

ALLIANCE will ensure that its data is findable through persistent identifiers (PIDs), such as Digital Object Identifiers (DOIs), which unambiguously identify the data and facilitate data citation. The data will be deposited in trusted repositories such as Zenodo, which assigns DOIs. The data will have rich metadata which will support findability, citation, and reuse.

Metadata will provide important context for the interpretation of the data and make it easier for machines to conduct automated analysis. Indicatively the following metadata schemes will be followed: Dublin Core, CERIF, DDI (general data). Open data standards will be used when possible, including the ones that will be used for captured data. The generated data will be well-documented and they will have clear license and provenance information.

A naming convention will be used to identify datasets associated to the project. This format is yet to be finalised, but will follow a clear convention that contains: the status of the dataset (raw, processed, calculated); an identifier of the country or geographic region; the institution to which the author of the data is affiliated; a short description (two to three words, concatenated using camel case); the project acronym; and a version number. The version number is structured as are version numbers for software: MAJOR.MINOR.PATCH (e.g. 1.02.03). Uploads to Zenodo of new versions should be done, where possible, under the same DOI as the original version.

3.2 Making data openly accessible

ALLIANCE aims to make research data openly accessible, following the Open Research Data Pilot, in which the project declares its intention to participate.

Open data standards will be used when possible, including community-agreed schemas, controlled vocabularies, keywords, thesauri, or ontologies where possible to ensure interoperability and integration with other data, applications, and workflows. The generated data will be well-documented, with clear license and provenance information. A README file will be created to ensure that the data can be correctly interpreted and re-analyzed by others.

Data storage and archiving will be performed in a secured form, with data encrypted using a strong cryptographic protocol, in servers indicated by the pilots or the technology providers, and agreed upon within the consortium. This is further detailed as part of T1.4 activities.

In summary, ALLIANCE will make data openly accessible by depositing it in trusted repositories with PIDs, rich metadata, well-documented, clear license, and provenance information.

3.3 Making data interoperable

ALLIANCE aims to integrate data and information from diverse disciplines and domains to achieve a shared understanding of data within the project. To accomplish this, ALLIANCE will adopt the Dublin Core Metadata Element set vocabulary as a standard to describe physical or

digital objects, following the standard ISO 15836. We will prioritize the use of open standards for interfaces to ensure maximum interoperability of the data. ALLIANCE intends to align with interoperability standards set forth by the European Common data spaces, which are integral to the European digital strategy.

To make ALLIANCE's data interoperable, the project will use community-agreed schemas, controlled vocabularies, keywords, thesauri or ontologies wherever possible. These standards help to ensure that data can be integrated with other data, applications, and workflows.

3.4 Increase data re- use (through clarifying licences)

ALLIANCE aims to increase data re-use through the use of clear licenses that govern the terms of data reuse. The project will use Creative Commons licenses[8], specifically the Attribution (CC BY) license and Creative Commons Zero (CC0) license. These licenses provide a standardized way to communicate how data can be used, reused, and shared.

The Attribution (CC BY) license allows others to distribute, remix, adapt, and build upon the licensed work, including for commercial purposes, as long as they give credit to the original creator. This license encourages maximum use and sharing of licensed material while still protecting the creator's rights. The Creative Commons Zero (CC0) license, on the other hand, waives all rights and places the licensed work in the public domain. This license allows for maximum reuse, remixing, and sharing without any restrictions.

ALLIANCE acknowledges the importance of ensuring the longevity of its datasets, particularly those that will be made openly accessible for future research purposes. To address this, the project will establish a data management framework that ensures that the datasets are stored in a secure and sustainable manner. The data will be stored in servers indicated by the pilots or technology providers, and agreed upon within the consortium. The use of trusted repositories will also enable the long-term use of the project’s data.

8 https://creativecommons.org/

4 Allocation of resources

ALLIANCE incurs both direct and indirect costs for data curation, storage, archiving, re-use, and management within a secure environment, including IT infrastructure and staff time. To avoid additional IT costs, ALLIANCE has selected repositories that are free of charge, such as the Zenodo repository used for making datasets and research outputs FAIR, and the ALLIANCE OneDrive facility used to host anonymized datasets internal to the project partners. UTH supports the costs for OneDrive as institutional costs, with no separate charge to ALLIANCE. The project coordinator, with the support of a Data Management Officer, is responsible for managing data within ALLIANCE.

5 Data Privacy and Ethics in Food Technology and Blockchain

Data acquisition, management, and privacy are important considerations in the context of food technology and blockchain.

Food technology often involves the use of sensors, internet of things (IoT) devices, and other digital technologies to collect and analyze data related to food production, distribution, and consumption. This data can include information about the quality and safety of food products, as well as information about consumer preferences and behavior. Effective data acquisition practices involve ensuring that data is collected in a responsible and transparent manner, with appropriate measures in place to protect the privacy and confidentiality of individuals.

Data management is also important in the context of food technology and blockchain. Blockchain technology has the potential to revolutionize the way that food supply chains are managed by enabling secure, transparent, and decentralized record-keeping. This can improve traceability, reduce fraud, and enhance food safety. Effective data management practices involve ensuring that data is stored, processed, and shared in a responsible and transparent manner, with appropriate measures in place to protect against unauthorized access or misuse.

Privacy is another key consideration in the context of food technology and blockchain. The use of digital technologies to collect and analyze data raises concerns about the privacy and confidentiality of individuals. Effective privacy practices involve ensuring that data is collected and used only for its intended purpose, with appropriate measures in place to protect against unauthorized access or disclosure. This includes obtaining informed consent from individuals for data collection and use, as well as ensuring that data is stored and processed in compliance with relevant privacy regulations.

Effective data acquisition, management, and privacy practices are essential for building trust and credibility in the food technology and blockchain industries, while also ensuring that individual rights and privacy are respected.

Moreover, in food technology, the use of data to track food from farm to table can raise privacy concerns as it involves the collection and processing of personal data, such as location data of farmers and food processing plants, which may be sensitive information. Additionally, the use of technology to monitor food safety and quality may involve the collection of health data related to food-borne illnesses, which must be protected in accordance with data privacy laws.[9]

In blockchain, privacy concerns can arise due to the public nature of the technology. Blockchain is designed to be transparent and immutable, which means that any data stored on the blockchain is visible to anyone. While this may be beneficial for some applications, it can be problematic when it comes to sensitive information, such as personal data. There is a risk that personal data could be exposed or stolen if proper security measures are not in place. Additionally, the use of blockchain to store personal data may be subject to data privacy laws, which can create compliance challenges.

Food technology and blockchain both have significant implications for data and privacy issues such as:

Data collection and sharing: Food technology can involve the use of sensors, mobile apps, and other tools to collect data on food products, such as their origin, quality, and safety. This data can be shared across the supply chain, from farmers to retailers, and even to consumers.

9 Liu, Z., et al. (2021). Privacy-preserving and verifiable food traceability system based on consortium blockchain. Information Sciences, 572, 47-60

However, the collection and sharing of this data can raise concerns about privacy, particularly if personal information is involved.

Traceability and transparency: Blockchain technology can be used to create a decentralized and tamper-proof record of a food product's journey from farm to table. This can help improve traceability and transparency in the food supply chain, which can be beneficial for food safety and quality. However, this also means that personal information may be stored on the blockchain, which raises privacy concerns.

Smart contracts: Blockchain technology can also be used to create smart contracts, which are self-executing contracts that automatically enforce the terms of an agreement. In the food industry, this could mean that farmers and suppliers agree to certain quality standards, and smart contracts automatically enforce these standards. However, smart contracts may also involve the sharing of personal information, which can raise privacy concerns.

Decentralization: Blockchain technology is often associated with decentralization, meaning that there is no central authority controlling the network. While this can be beneficial for security and transparency, it can also make it more difficult to control the use of personal information.[10]

Overall, data and privacy issues are significant concerns in both food technology and blockchain. As these technologies continue to evolve and become more widespread, it will be important to address these concerns and ensure that personal information is protected.

10 Wang, S., et al. (2019). Blockchain in the food industry: A review. Trends in Food Science & Technology, 91, 14-23

6 Data security

The Zenodo repository, which will be used for publishing and maintaining final project outcomes, deliverables, and scientific publications, is hosted at CERN and it is subject to its rules for data security, as reported at https://zenodo.org/policies.

Moreover, the ALLIANCE website and its respective servers will be used as a repository to store some data.

The ALLIANCE OneDrive is a file hosting service under Microsoft Teams, provided by UTH, that gives the possibility to all partners to share documents, request inputs from other partners and work together on draft deliverables using Office online.

In the shared folder, the following folders have been created:

- **Deliverables Submitted**: contains all the final version of the submitted deliverables
- **Management:** it contains the final version of the GA, information about the payments. It also contains the final version of the CA and the templates
- **Meetings**: all necessary information about previous and upcoming meetings and confcalls.
- **Work Packages**: under the responsibility of each WP leader, there is one folder per each WP. It also contains subfolders for the different related deliverables
- **Dissemination**: a folder where the partners exchange information about the events to be attended.
- **Reporting**: it will be used to exchange information about the upcoming reports.

This shared folder is a living tool and it will evolve based on the evolution and the needs of the project.

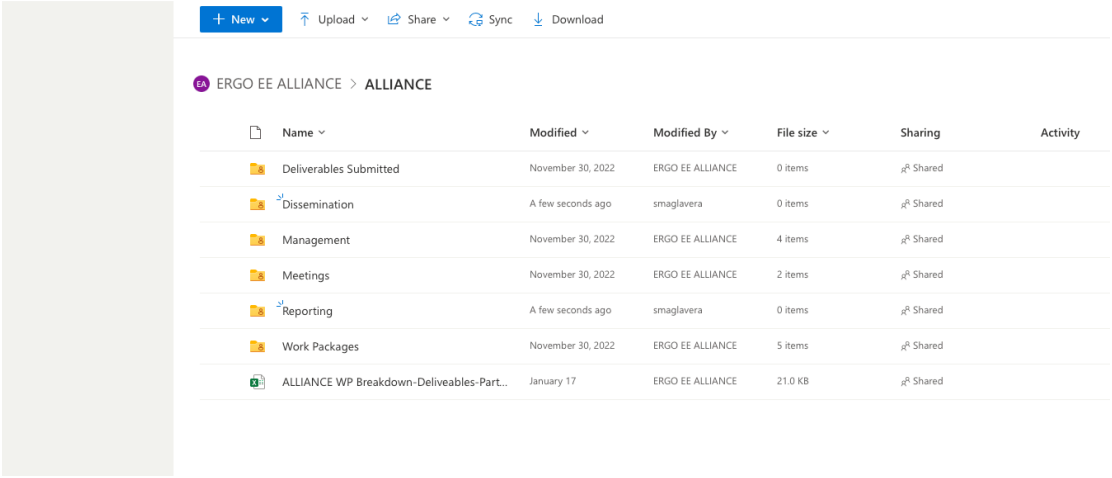

Figure 2 – ALLIANCE OneDrive [11](shared folder)

Data in OneDrive is encrypted and access to the ALLIANCE One Drive is reserved to authorised persons, invited by the manager of the OneDrive instance. Access is user name and password authenticated, and as a standard dual- factor authorisation for access is activated. Access to specific folders created within OneDrive can be assigned to a specific group of users, or to a

11 ALLIANCE | D1.1 - Project Management Handbook

user individually. A sharable link can also be created to share the dataset with a third- party user, without access to the instance of OneDrive.

For each folder as well as files within a folder, the following access privileges can be granted. Note that access rights are inherited by sub- folders:

- Share: when enabled this allows a sharable link (URL) to a file or folder to be created
- Read: user has read access to the file or folder
- Edit: user can modify a file or folder
- Create: user can create a new folder or file (but not delete)
- Delete: user can delete a file or folder

7 Legal and Ethical Aspects

The European Union (EU) has a legal framework that governs the use of blockchain technology in the food industry. Here are some of the key regulations and guidelines

General Data Protection Regulation (GDPR)[12]: The GDPR is a regulation that governs the collection, use, and storage of personal data in the EU. It applies to blockchain-based systems that collect and process personal data, and requires that data controllers ensure that the data is processed in a lawful, transparent, and secure manner.

General Food Law Regulation (EC) No 178/2002[13]: This regulation establishes the general principles and requirements of food law in the EU, including traceability and transparency in the food supply chain. Blockchain-based systems can be used to enhance traceability and transparency, and must comply with the requirements of this regulation.

Novel Food Regulation (EU) 2015/2283[14]: This regulation establishes the procedures for authorizing and placing novel foods on the EU market. Blockchain-based systems can be used to ensure compliance with these procedures, and to enhance traceability and transparency in the supply chain of novel foods.

European Food Safety Authority (EFSA) Guidance[15]: The EFSA has issued guidance on the use of blockchain technology in the food industry, which provides recommendations on data protection, security, and transparency.

Digital Single Market Strategy[16]: The EU's Digital Single Market Strategy includes initiatives to promote the development and adoption of blockchain technology in the EU, including the creation of a European Blockchain Partnership to develop cross-border blockchain applications.

These regulations and guidelines provide a framework for the use of blockchain technology in the food industry in the EU. However, as the technology is still developing, there may be further regulatory developments in the future.

The EU-UK adequacy decision was granted on June 28, 2021, and it allows for the free flow of personal data between the EU and the UK without additional safeguards or legal barriers. This means that personal data can be transferred from the EU to the UK and vice versa, without the need for specific agreements or contracts.

Internationally, there is no specific international legal framework for food technology and blockchain. However, there are some international organizations and initiatives that address issues related to food safety, quality, and traceability, which are relevant to the use of blockchain technology in the food industry including The Food and Agriculture Organization (FAO) of the United Nations, the Global Food Safety Initiative (GFSI, the Blockchain for Social Impact Coalition (BSIC).

While there is no international legal framework specifically for food technology and blockchain, these organizations and initiatives provide guidance and standards that can inform the development and implementation of blockchain-based solutions in the food industry.

12 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

13 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002R0178

14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015R2283

15 https://www.efsa.europa.eu/en/methodology/guidance

16 https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html

7.1 ALLIANCE's Compliance

ALLIANCE is committed to conducting research activities in accordance with the European and International accepted ethical principles, scientific best practices, and applicable laws. The research will adhere to the national legal and ethical requirements of the participating countries where potential ethical issues arise.

One of the primary ethical considerations is the protection of personal data and privacy. The project is committed to protecting the personal data of all project participants and ensuring that it is handled in accordance with applicable data protection laws, such as the EU General Data Protection Regulation (GDPR). ALLIANCE has put in place appropriate safeguards to ensure that personal data is only collected and processed for legitimate purposes and is not shared with third parties without the necessary consent.

Another ethical consideration is ensuring that the research conducted by the project is carried out in an ethical and responsible manner. This includes ensuring that the research is conducted with the highest standards of integrity and professionalism and that any potential risks or harm to human subjects are minimized. The project has a code of ethics that outlines these principles and provides guidelines for ensuring that all research is conducted in accordance with ethical standards.

ALLIANCE will collaborate with citizens, decision-makers, and other stakeholders. Adult participants who are fully informed and able to give prior consent (Appendix 1 - Consent Form) will be involved in project activities. ALLIANCE will provide detailed information about project objectives, methods, and specific activity details, and participants will be treated with respect and equity.

To ensure compliance with research ethics, ALLIANCE will create a document to log all project activities and assess compliance with research ethics. This document will be regularly updated throughout the project to ensure ongoing compliance. The document will outline the ethical considerations of the project and provide guidelines for researchers to follow. Additionally, in case ethical or legal issues arise during the project, the consortium will establish an ethics committee. This committee will be responsible for reviewing and approving all research activities to ensure compliance with ethical and legal standards, if needed so.

ALLIANCE will collect minimal personal data from participants, such as name, gender, email contact, and representation. This data will be used only with consent for project activities and stored in a restricted access, access-controlled partition of the collaborative platform. ALLIANCE will adhere to the "do no harm principle" and "anonymization principle" when analyzing data and producing outputs such as publications, media reports, and climate services products.

As ALLIANCE has a UK partner, the adequacy decision which was mentioned as above, ensures that the project can transfer personal data between the EU and the UK without any issues. Additionally, as of now, there are no plans for ALLIANCE project partners to exchange personal data with partners based in Serbia and Turkey (non-EU partners), which will abide by the relevant national regulations for these countries and adhere to their research ethics and integrity guidelines.

However, there may be a need for the exchange of non-personal data between partners for the purpose of conducting research activities as part of ALLIANCE.

Non-personal data refers to data that does not identify individuals and is therefore not subject to data protection regulations in the same way that personal data is. This could include data such as traffic flow data, weather data, or infrastructure data.

In any case, before any data exchange takes place, it is important for the partners to ensure that appropriate safeguards are in place to protect the confidentiality, integrity, and availability of the data, in line with the relevant data protection regulations and best practices.

The research is exclusively focused on civil applications and is not expected to lead to risks of misuse, stigmatization of certain societal groups, political or financial retaliation. The project will comply with relevant national regulations for Demonstrators outside the EU, and no personal information will be shared beyond these Demonstrators without the participants' consent.

ALLIANCE aims to share benefits emerging from project activities among project partners, citizens, stakeholders, and decision-makers in Demonstrators and beyond. Participants will benefit from research results shared through various dissemination activities appropriate for end-user capacity and access.

8 Fundamental Rights Consideration

The fundamental rights in the European Union are outlined in the Charter of Fundamental Rights [17]which includes the human dignity when everyone has the right to dignity, and no one shall be subjected to inhumane or degrading treatment, the freedom of thought, conscience, and religion, as well as freedom of expression, assembly, and association, the equality when everyone is equal before the law, and discrimination based on any ground is prohibited.

The Chapter of Fundamental Rights refers also to solidarity as the EU is founded on the values of solidarity and mutual assistance among its member states and to citizens' rights as all EU citizens have the right to move and reside freely within the EU, to vote and stand as candidates in European and local elections, and to receive protection from the diplomatic and consular authorities of any EU country when in a non-EU country. Everyone has the right to a fair trial and the presumption of innocence, as well as the right to legal aid and to access to justice and everyone has the right to respect for their private and family life, home, and communications.

The protection of personal data [18]is a fundamental right as everyone has the right to the protection of their personal data, the freedom of business and the consumer protection.

These fundamental rights are legally binding on the institutions, bodies, and agencies of the EU, as well as on the member states when they are implementing EU law.

Following the above, it is forehead to mention that there are no specific fundamental rights regarding in food technology and blockchain, as these are relatively new and emerging fields that do not have well-established legal frameworks. However, there are several rights and principles that are relevant to the intersection of food technology and blockchain, including:

- Right to privacy: Individuals have the right to control their personal data and to know how it is being used, particularly in the context of blockchain-based systems that involve the collection and sharing of data.
- Right to transparency: Consumers have the right to know where their food comes from, how it was produced, and how it was transported and stored. Blockchain-based systems can provide greater transparency in the food supply chain by allowing consumers to track the journey of their food from farm to table.
- Right to food safety: Consumers have the right to safe and healthy food. Blockchain-based systems can help ensure food safety by allowing for more efficient tracking and recall of contaminated or unsafe products.
- Right to fair labor practices: Workers in the food industry have the right to fair wages, safe working conditions, and freedom from exploitation. Blockchain-based systems can help ensure fair labor practices by providing greater transparency and accountability in the supply chain.
- Right to food security: Everyone has the right to access sufficient, safe, and nutritious food. Blockchain-based systems can help ensure food security by improving efficiency and transparency in the food supply chain, and by reducing food waste.

All these rights and principles are important considerations in the development and implementation of blockchain-based solutions in the food industry. By prioritizing these values, we can work towards a more transparent, secure, and equitable food system for everyone, trying to avoid several issues.

17 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

18 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Issues regarding fundamental rights in food technology and blockchain can arise due to the collection, use, and management of personal data. For example, the use of blockchain technology in food supply chains can involve the collection and sharing of sensitive information such as product origins, handling, and storage. If this data is not handled in a secure and transparent manner, it can lead to privacy violations and potential breaches of fundamental rights.

To be proactive in addressing these issues, it is important to adhere to relevant laws and regulations such as the GDPR and ensure that proper consent and data protection measures are in place. This includes implementing appropriate security measures, such as encryption and access controls, and ensuring that individuals have control over their personal data and are informed about how it is being used.

In addition, it is important to consider ethical principles such as transparency, accountability, and fairness when designing and implementing food technology and blockchain systems. This can involve involving stakeholders in the design process, conducting privacy impact assessments, and being transparent about how data is collected, used, and shared. By taking a proactive approach to fundamental rights and privacy issues, we can ensure that food technology and blockchain are used in a way that respects individual rights and freedoms.

This Deliverable (D1.2) outlines the project's commitment to upholding ethical principles, internationally accepted scientific best practices, and applicable international and EU law to ensure high-quality research and enterprise culture with the highest possible standards of integrity and practice. This chapter explains how the research ALLIANCE undertakes meets the national legal and ethical requirements of the participating countries in which tasks raising potential ethical issues are to be conducted. It also outlines how the project complies with Decision No. 2013/743/EC, recognizing the Charter of Fundamental Rights of the EU, adherence to ethical principles. Additionally, the project's approach is to work with citizens, decision-makers, and other stakeholders in the seven Demonstrators, including the limited personal data collected from adult participants and how it is stored and used.

In ALLIANCE it is well know how important is to be proactive in addressing potential violations of fundamental rights in the field of food technology and blockchain by implementing appropriate safeguards and regularly reviewing data management practices to ensure compliance with EU regulations, legal frameworks, and ethical principles. Here are the general steps that could be taken during ALLIANCE:

1. Identify the violation: The first step is to identify the violation of the fundamental right that has occurred. This could involve reviewing the specific EU regulations, legal frameworks, and ethical principles that have been violated.
2. Document the violation: It's important to document the violation, including the specific details of what happened, who was involved, and any evidence that can support the claim.
3. Report the violation: Depending on the severity of the violation, it may be appropriate to report it to the relevant authorities, such as data protection authorities, regulatory bodies, or law enforcement agencies.
4. Take corrective action: Once a violation has been identified and documented, it's important to take corrective action to prevent similar violations from occurring in the future. This could involve changes to the technology or data management practices, as well as implementing additional safeguards to protect fundamental rights.

To sum up, ensuring fundamental rights and societal values are upheld is crucial for the success of ALLIANCE. It is important for all partners to remain aware of these rights and values throughout the project's lifespan, from establishing user requirements to designing and implementing the technology, and beyond. This deliverable has highlighted key legal

instruments that protect human rights, as well as ethical, privacy, and data protection principles. These principles must be integrated into the food technology and blockchain system and its deployment. It is imperative to identify and address any ethical, privacy, and data protection challenges at the earliest stage possible to minimize harm. Future consequences and impacts of proposed actions must also be considered in relation to human rights and societal values.

APPENDIX 1

The following Consent Form template will be used to facilitate data exchange between the project partners and stakeholders providing data. This template is also provided as a stand-alone document on the ALLIANCE OneDrive. This template may be amended to suit the local context, including translation into a more appropriate language if suitable. Note also that the template that is available on the ALLIANCE OneDrive will be refined in the course of the project and the template below reflects status as the time of writing this DMP. It is recommended that when establishing a Consent Form the template file from the ALLIANCE OneDrive is used, and amended when required to suit the local context.

Consent Form

Project Acronym: ALLIANCE

Project Full Name: A holistic framework in the quality Labelled food supply chain systems' management towards enhanced data Integrity and veracity, interoperability, transparency, and traceability

Grant Agreement: ALLIANCE project has received funding from the European Union's HORIZON-CL6-2022-FARM2FORK-01 call under grant agreement No 101084188

Project Duration: 36 Months (1/11/2022-31/10/2025)

1. INTRODUCTION

You are invited to take part in a research activity within the ALLIANCE project in the form ..... Please read this document carefully before deciding whether you will participate or not. We encourage you to ask all the questions you may have; it is important that you understand all the proceedings, including possible risks and benefits. This informed consent document may include words that you do not understand. If this is the case, please ask the project representative to fully explain the meaning of the word or piece of information you do not accurately understand. At all times, we assure compliance with the current legislation.

2. PURPOSE OF THE PROJECT

The overall objective of the ALLIANCE project is to represent a paradigm shift in the Food Supply Chain Systems' management for the combat against Food Fraud, distinguishing from the traditional approaches that leverage monolithic digitalized logistic solutions and standalone FSC interoperability protocols. ALLIANCE aims to provide a holistic framework that safeguards data integrity and veracity, enhances traceability and transparency, and reinforces interoperability in the quality-labeled supply chain of organic, PDO, PGI, and GI food, through innovative technology solutions and validated approaches (such as distributed ledger technologies supported by IoT sensing devices, providing extensible anchors to interoperability protocols and use of in-situ portable rapid testing devices to detect adulteration and verify food origin and authenticity) and fosters evidence-based decision making through AI and ML for preventative interventions and actionable planning. The proposed framework will improve the social and economic sustainability of quality-labeled food supply chains by ensuring quality &

authenticity, and increasing food safety, while also considering the climatic and environmental impacts of food products. The technologies to be employed in this project will be described and demonstrated in detail to reach higher technology readiness levels (TRLs) and enable smooth and rapid adoption by all stakeholders.

3. CONFIRMATION

You can participate in this project activity by signing this consent to authorize us to use the data you provide and treat them as confidential and anonymous.

I hereby declare:

- *I am 18 years or older and I am competent to provide consent. I am fully informed about the aims of the project and this particular activity and I understand that there is no compulsion to participate in the project's activity. I understand that I may withdraw my participation at any stage;*
- *I understand the document providing information about this research and this consent form. All my questions have been answered to my satisfaction;*
- *I understand and agree that my data and input (e.g., collected through this meeting) are used for scientific purposes; I have no objection that my data being published in scientific and official project publications in a way that does not reveal my identity;*
- *I confirm that irrevocably and for an unlimited period of time and space all rights for any use and publication of the video material and/or photographic material produced by the ALLIANCE project partners during the ..... in INSERT DEMONSTRATOR CITY/REGION NAME HERE will be transferred from me to the project partners and may only be used within the scope of the public presentation of the project partners and the ALLIANCE project. I waive any payment of fees in any form and make no claims whatsoever. The naming of the people photographed is at the discretion of the ALLIANCE project partners.*

I have received a copy of this agreement. This consent form is made pursuant to the relevant national, and European data protection laws, regulations, and personal data treatment obligations.

Name and surname of participant:

.....

Place, date, and signature of participant:

.....

Statement of investigator's responsibility:

I have explained to the potential participant the aims and objectives of this project, the procedures to attend, and any possible risks or inconveniences. I have offered to answer any questions and fully answered such questions.

I believe that the participant understands my explanation and has freely given informed consent.

Name and surname of the researcher:

……

Place, date, and signature of the researcher: .....

APPENDIX 2

The following template will be used to facilitate data exchange between the project partners and stakeholders providing data. This template is also provided as a stand- alone document on the ALLIANCE OneDrive in the Project Resources folder. This template may be amended to suit the local context, including translation into amore appropriate language if suitable. Note also that the template that is available on the ALLIANCE OneDrive will be refined in the course of the project and the template below reflects status as the time of writingthis DMP. It is recommended that when establishing a data sharing agreement the template file from the ALLIANCE OneDrive is used, and amended when required to suit the local context. Note also that this data sharing agreement is applicable to proprietary data, as for open data, a data sharing agreement is not needed.

ALLIANCE Research Agreement

Parties

A. Partner A ....., org. No....., address .....,

and
B. Partner B ....., org. No. ....., address .....,

A- B are hereinafter collectively referred to as “Parties”, and individually as “Party”

Background

Partner A is involved in the ALLIANCE project funded by European Research Executive Agency (REA), call “Farm to fork, Communities Development and Climate Action”, Grant agreement 101084188 (as further described below, the “Project”).

One of the purposes of the Project is to ...

If applicable, state the organisations that will get access to the data via Partner A (the Project Members”)Add scientific rationale for the data exchange.

Parties therefore enter into this research agreement, which includes this background, in order to specify rightsand responsibilities.

Article 1, Partner B's obligations

State Partner B's obligations: dataset, variables, period etc. to be extracted.

Article 2, Partner A's obligations

State Partner A's obligations.

Article 3, Payment

No monetary payment is involved in this agreement.

Article 4, Agreement Conditions, Data Licence and Data Management

Add conditions, data licence requirements etc. For example:

***Partner A** is granted a limited licence to use the Data in the Project. **Partner A** is granted a right tosub- license the Data to the Project members in accordance with the limitations stated in this Article*

*The Data shall only be used by **Partner A** and the Project members stipulated in this Agreement. The Data shall only be used within the Project and must, in all its existing forms and copies generated, be destroyed after Project ending.*

***Partner B** shall be offered to participate as co- author in all publications based on the Data. **Partner A** or the aforementioned Project members should make direct contact on this matter with Contact Information.*

***Partner B** makes no representation and gives no warranties about the Data and any reliance on themby **Partner A** or any Project member will be at their own risk.*

The Data should be referred to in publications by citing the following papers:

- *Paper A...*
- *Paper B...*

Article 5, Amendments

Amendments to this agreement shall be made in writing and agreed between the Parties.

Article 6, Miscellaneous

Matters related to this Agreement, such as practical arrangements regarding the delivery of Data, shall be discussed and decided upon in a cooperative spirit. Neither Partner would hold the other liable to litigation due to this agreement. Differences or conflicts arising as a result of a breach in the agreement are to be resolved through dialogue.

Article 7, Contacts

The following people are the designated contact points for this Agreement:

Partner B

The contact for scientific work related to this agreement is Contact information. The administrative contact for this agreement is Contact information.

Partner A

The contact for scientific work related to this agreement is *Contact information.* The administrative contact for this agreement is *Contact information.*

Article 8, Entry into force

This Agreement shall enter into force when signed by both Parties and shall regulate the time periodequivalent of the Project time period.

Place, Date *Signature*	*Place, Date* *Signature*
Name, Title *Position* *Department* *Affiliation* *Telephone* *Email*	*Name, Title* *Position* *Department* *Affiliation* *Telephone* *Email*

APPENDIX 3

Data types, size, sources and management per Partner

Partner	Data collected	Data Type and size	Tool/Technology	Personal data (yes or no)
BioCoS	Samples of olive leaf and olive oil	DNA data (numerical), geolocation of the samples, .csv and .docx files, 500MB	Data collected from systems, qPCR-HRM molecular analysis device	Yes
LGL	Samples of olive leaf and olive oil	DNA data (numerical), .csv and .docx files, 500MB	qPCR-HRM molecular analysis device	No
RMS	Information about production system	General Data (name, address, identification number, laboratory analysis, scope of production, volume i.e. quantity produced, purchased and sold, PDF, Excel files, 100-200MB	Laboratory analysis	Possible collection of personal data
Alce Nero SpA	Samples of flours and pasta	Chemical data, physical data (eg. Pressure, temperature), PDF, Excel files	-	Yes
ASINCAR	Technical data linked to the experiments needed for the development of the foreseen applications	Store technical data linked to the experiments needed for the development of the foreseen applications, .CSV, .TXT, .XLSX, .PDF, .DOC, .JPEG, .PNG Size expected will be ca. 1 TB	Use of the NIR, HSI sensors, perform the lab analysis	No
CIHEAM-IAMM	Production data, economic data, and socio-demographic data	Questionnaires	-	No
FederBio Servizi	Technical data	Technical data	-	Possible collection of personal data

Migros Tic. A.S.	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form.	-	No
UNIBO	Personal data	Personal Data, the data format will be in sav, xls, csv format.	-	Yes
University of Thessaly	Technical data	Logs, code, usability information, data from digital smart contracts and geolocation information, .txt raw data format	IoT devices	Yes

Partner	Data source	Personal data	Data Storage
BioCoS	Molecular analysis from the pilot testers, short sample collection form	contacts of the responsible people, geolocation information	Local computer (first collection phase), then in SSD drives and on cloud
LGL	Molecular analysis of olive leaf and olive oil samples	-	Local computer (first collection phase), then data will be backed-up on LGL server
RMS	Field visits, which include interviews, documents reviews, visual evidence etc.	The data collection may include personal data of an individual(s)	Data stored on-line (on Sharepoint location) and external hard-disk while back-up is regularly done
Alce Nero SpA	Analytical tests, analysing different kind of samples	Personal data of technical people enrolled in production of flours and pasta	Drive collector
ASINCAR	Main research methods will be common prototyping (test-fail/success) and piloting practices	-	ASINCAR server
CIHEAM-IAMM	Data will be collected directly from the involved stakeholders via personal interviews by the use of questionnaires	-	In the cloud of ALLIANCE
FederBio Servizi	Data will be collected from the involved stakeholders via	Personal data might be collected through surveys to be	Data will be stored in FBS's cloud repository (Google Drive)

	interviews, surveys, workshops, webinars, participation in pilots	conducted in Task 3.6 - Consumer Demand Assessment and Strengthening	
Migros Tic. A.S.	-	-	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form. Migros is not asked to share retail data either. However, we consider that such necessity can rise during the project and set forth the rules for data sharing in DESCA.
UNIBO	Indirectly with the use of a consumer marketing research agency	Personal data from research participants (questionnaire and signed consent forms). Questionnaires will be processed anonymously and in aggregate form	The data will be stored in online electronic archives. The data will be stored in the Unibo cloud system dedicated to the Alliance project (teams, sharepoint)
University of Thessaly	Data will be gathered through the demonstration of Pilots during the operation of the Alliance platform. The collection of the data will be conducted through the use of IoT devices or they can be provided as an input by the end-users	Personal data stemming from digital smart contracts, geolocation information for the identification of food fraud incidences	In the Blockchain repository, that will be hosted in the UTH's cloud infrastructure

Partner	Data retention	Security	Access
BioCoS	At least five year after the end of the project	Regular back-up of the files, password-protected file sharing, ML/AI implementation for the development of the blockchain system	From BioCoS, access will be granted for Dr. Dourou, Dr. Arhondakis, MS Lampropoulou and MS Moraiti. Regarding the project, information will be shared with the partners of the WPs that BioCoS is actively involved – mainly WP3 and WP4
LGL	At least five year after the end of the project	Daily back-up of the files on LGL server, access control by LGL, password-protected file sharing to ensure that the accessibility of the data is secured	From LGL, access will be granted for Dr. Ulrich Busch, Dr. Ingrid Huber, Dr. Patrick Guertler, Dr. Gabriele Zeiler-Hilgart and the project stuff tom be hired (NN). Regarding the project, information will be shared with the ALLIANCE partners of the WPs that LGL is actively involved – mainly

			WP3 and WP4, LGL IT department
RMS	At least five year after the end of the project	Files backed-up securely on Sharepoint, with limited accessability, as well as on external hard-drive with password protection	Access to different documents is defined for different members of RMS – some of them have access to all the data, some of them only partly access, in line with their role in the certification process. Regarding the project partners, there will be some information exchange with Original and Institute for Food Technology (FINS) about mutual project activities (in relation to traceability of products in the supply chain and simple tests for determining the "Arilje raspberry")
Alce Nero SpA	At least one year after the end of the project	Use of anonymous by use of alphanumerical codes	Enrolled researchers of the company, other project partners
ASINCAR	At least five year after the end of the project	ASINCAR server that has already implemented common high standards about data security and privacy	ASINCAR staff involved in ALLIANCE
CIHEAM-IAMM	As long as it is required	Via anonymous questionnaires	All the involved partners
FederBio Servizi	As long as it is required	The data will be stored in the company cloud repository which is password protected	FBS staff will have access to data, that will be used to draft reports/documents which will be made available to WP coordinator/project partners in order to implement project activities and achieve project deliverables

Migros Tic. A.S.	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form. Migros is not asked to share retail data either. However, we consider that such necessity can rise during the project and set forth the rules for data sharing in DESCA.	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form. Migros is not asked to share retail data either. However, we consider that such necessity can rise during the project and set forth the rules for data sharing in DESCA.	In the course of the project, Migros is not responsible of storing and maintaining other partner's data in either a structured form or semi-structured form. Migros is not asked to share retail data either. However, we consider that such necessity can rise during the project and set forth the rules for data sharing in DESCA
UNIBO	Until the end of the project. Personal data will be kept for a period of time not exceeding the achievement of the purposes for which they are processed. The open data will be stored in Zenodo.	The data are stored in a Unibo cloud system, with access control and password-protected, the data will be processed anonymously and in aggregate form	The members of the Unibo team will have access to the data
University of Thessaly	The data will be kept during the project execution and for a period of six-month after the project finalisation	Strong password policy, two factor authentication and multifactor authentication schemes, monitoring user's activity keeping and analysing logs and use of rule-based alerts that inform system's administrators for suspicious activity patterns, strong network policy using vpn and firewall will be implemented, data masking techniques	Researchers, developers, operators and testers and the ALLIANCE consortium that wish to use the platform. Their role will be identified during the project execution as well as their permissions and rights on accessing specific data and services