ALLIANCE

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

DELIVERABLE 1.5- MID-TERM 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: 30.04.2024

Version: 1

Versioning and contribution history

Version	Description	Contributions
0.1	The initial draft of the deliverable	WISE4
0.2	1st review of the deliverable	LGL
0.3	2nd review of the deliverable	LGL
0.4	3rd review of the deliverable	UTH
0.5	Internal Review	WISE4
1	Final version of submission	UTH

Authors

Author	Partner
Maria Kadena	WISE4

Reviewers

Name	Organization
Dr. Ingrid Huber	Bavarian Health and Food Safety Authority (LGL)
Dr. Frederic D.B. Schedel	Bavarian Health and Food Safety Authority (LGL)
Dr. Kostas Choumas	University of Thessaly (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

List of Figures

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
T	Task
UTH	University of Thessaly
LC	The Lisbon Council For Economic Competitiveness Asbl
ASINCAR	Asociacion De Investigacion De Industrias Carnicas Del Principado De Asturias

LGL	Bavarian Health and Food Safety Authority

Executive Summary

Deliverable D1.5 presents the second version of the ALLIANCE DMP, which is delivered on M18 of the project. The DMP is a living document during the whole lifetime of the project. The deliverable outlines how the data are collected, produced, and used within ALLIANCE. It also describes how these data are shared, accessible for reuse and further exploitation, and how they are curated, preserved, or deleted when necessary. The project has made sure to comply with GDPR and national regulations, while also following the FAIR principles, to handle the data legally and ethically.

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

Monitoring the status of the data regularly ensures 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 D1.2, are anticipated to remain intact until the end of the project.

1 Introduction

This DMP is a document that describes the data collected and generated by the ALLIANCE 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 current document outlines datasets and their analysis, providing details on how data has been managed and will continue to be handled within the project. It aims to maximize the availability of open and reusable data from the project to ease future reuse. Each dataset will be clearly defined, modified, and described, with information on its compliance with standards, and how it is accessible, interoperable, and reusable, along with details on data preservation and management practices.

This version is the second of three planned updates for ALLIANCE, with the final version (D1.3 Final Data Management Plan, Ethics, Fundamental Rights, Data and Privacy Issues) scheduled for delivery at month 36. The Final DMP is expected to include the full description of the data and metadata collected/processed and generated in the project, including their corresponding post-project dissemination and exploitation plans. Finally, the guidance from the initial DMP to ALLIANCE members remains in force also with this updated DMP: they should keep the list of collected/processed datasets up to date during project implementation.

The document is structured as follows:

- Chapter 2 - Data Summary: Data Management Components in each WP.
- Chapter 3 - FAIR Data Management: description of how ALLIANCE implements the FAIR (Findable, Accessible Interoperable, and Re-usable) principles
- Chapter 4 - Allocation of resources: description of associated costs and personnel
- Chapter 5 - Ethical aspects: how personal and sensitive information remain duly protected
- Chapter 6 - Data security: how the security of data will be ensured
- Chapter 7 - Legal and Ethical Aspects
- Chapter 8 - Fundamental Rights Consideration
- Appendix 1- Template Consent Form
- Appendix 2 - ALLIANCE Research Agreement
- Appendix 3 – Data types, size, sources, and management per Partner

2 Data Summary: Data Management Components

2.1 DMP Components in WP1 - Project and Technical Management (UTH)

Data Summary	Contact details of the project partners. Databases containing all the necessary information regarding the project partners. The project partners' data are stored on a simple table (excel file) and it is stored in the ALLIANCE SharePoint folder, with the following fields: • Organisation • Name • Email Furthermore, consortium meetings have been conducted remotely every month to discuss the project's progress and address any important issues. Most of the meetings have been conducted using Google Meet or Teams. Meetings have been prepared after each meeting and are stored in the ALLIANCE SharePoint folder (docx. format). Moreover, WP leaders have sent input on how they handle and process the data produced/generated and/ or collected during the project. Presentations, agenda, and the participants list of each plenary meeting or review meeting have been collected and kept. Lastly, three project events have been held; the first one was the kick-off meeting of the project on 19-20/12/2022 in Volos, Greece, the second one was on 5-6/9/2023 in Bologna, Italy and the third one was on 9-10/4/2024 in Athens, Greece. The aim of these meetings was to be informed about the project status and progress, as well as to be better coordinated for the future of the project. The material of these meetings (agenda, presentations, recordings) is stored in the project's SharePoint folder.

Making data findable, including provisions for metadata`	The data with regards to the meetings are stored on a server that is located in the facilities of the coordinator (UTH), and specifically, in the ALLIANCE SharePoint folder. The data are not directly accessible from outside. Moreover, these data will not be made available to third parties. However, input provided concerning the data management is available through the respective deliverables (D1.2 Initial Data Management Plan, D1.5 Mid-term Data Management Plan). The dissemination level of these deliverables is public and they will be available on the project's website, SharePoint folder, and in Zenodo once they are accepted.
Making data openly accessible	The datasets are not publicly available. All the data will be publicly available as part of the aforementioned deliverables and through the ALLIANCE website, SharePoint folder, and Zenodo.
Making data interoperable	N/A
Increase data re-use	Data will be publicly available as part of the aforementioned deliverables and are accessed and re-used by third parties indefinitely without a license.
Allocation of resources	Resources have been allocated according to the project plan and WP1 allocated resources. No additional costs are foreseen for making this dataset FAIR.
Data security	The data are collected for internal use in the project, and not intended for long-term preservation. No personal information will be kept after the end of the project. Furthermore, WISE4 pays special attention to security and respects the privacy and confidentiality of the user's personal data by fully complying with the applicable national, European, and international framework, and the European Union's General Data Protection Regulation (GDPR) 2016/679.
Ethical aspects	N/A
Other issues	N/A

2.2 DMP Components in WP2 - Food Traceability (UTH)

Data Summary	WP2 – Food Traceability Data related to WP2 is stored on the WP2 ALLIANCE SharePoint folder in the following fields: • Deliverable: project partner data related to deliverable D2.3 is stored in this folder. • Monthly meetings (using Teams): consortium meetings have been conducted remotely every month to discuss the project progress and address any important issues. All presentations shown in these meetings are stored in this folder. • T2.1 - T2.5: technical data linked to the experiments/works carried out under the different tasks (5 tasks are included in WP2) is stored in the corresponding folders.
Making data findable, including provisions for metadata	The data with regards to the monthly meetings are stored on UTH´s server (WP leader), which has already implemented common high standards about data security and privacy, and in the ALLIANCE SharePoint folder (see previous row). The data are not directly accessible from outside and will not be made available to third parties. Inputs provided with regards to the deliverable D2.3 are available through the respective folder on SharePoint. The dissemination level of deliverable D2.3 will be public and it will be available on the project's website, in the SharePoint folder, and in Zenodo. As part of any stored data, metadata will be generated which will include sufficient information with appropriate keywords to help external and internal users locate data and related information

Making data openly accessible	The datasets generated in each task are not publicly available. All the data are publicly available as part of the aforementioned deliverable D2.3 and through the ALLIANCE website, Sharepoint folder, and Zenodo.
Making data interoperable	Outcomes from T2.2 will provide interoperability mechanisms for historical data or data generated by the developed FSCs.
Increase data re-use	Data are publicly available as part of the aforementioned deliverables and are accessed and re-used by third parties indefinitely without a license.
Allocation of resources	Resources have been allocated according to the project plan and WP2 allocated resources. No additional costs are foreseen for making this dataset FAIR.
Data security	The data are collected for internal use in the project, and not intended for long-term preservation. No personal information will be kept after the end of the project. Furthermore, WISE4 pays special attention to security and respects the privacy and confidentiality of the user's personal data by fully complying with the applicable national, European and international framework, and the European Union's General Data Protection Regulation (GDPR) 2016/679.
Ethical aspects	N/A
Other issues	N/A

2.2.1 Task 2.4 – AI-enabled Early Warning and Decision Support System (INTRA)

Data Summary	Anonymized time-series data from OLYMPOS, stored in the Blockchain provided by UTH, will be used for detecting early warning food fraud signals. Early warning signals will be integer values (as risk levels) or float numbers (as percentages). Risk factors mentioned will be combined with other qualitative or/and quantitative variables of intertest to construct a multi-criteria individual or/and group decision-making problem for recommendation purposes. Recommendations will be in an alphanumeric format. Data regarding decision makers will be needed especially to distinguish roles and

	responsibilities from a business point of view (e.g., manager, employee, etc.).
Making data findable, including provisions for metadata	INTRA will keep collected data in an internal database for supporting both early warning and decision support. Therefore, data will be fully findable.
Making data openly accessible	Early warning signals and recommendations will be provided to both UTH (for updating their blockchain) and FINS (for updating their knowledge data base).
Making data interoperable	INTRA API for the EWSDSS' outputs will be in a json format explaining both inputs given to EWSDSS and outputs obtained.
Increase data re-use	Yes. Data generated will be used from UTH to support ALLIANCE traceability and from FINS to compute descriptive statistics and dashboards of interest.
Allocation of resources	Project budget is sufficient to cover hosting costs and support ALLIANCE pilots.
Data security	Data will be accessible only from authorized users logging in EWSDSS portal. EWSDSS outputs will be requested through APIs only from certified users.
Ethical aspects	N/A
Other issues	N/A

2.3 DMP Components in WP3 - Food Safety and Authenticity (ASINCAR)

Data Summary	WP3 – Food Safety and Authenticity Data related to WP3 is stored on WP3 ALLIANCE SharePoint folder in the following fields: • Deliverable: project partner data related to deliverable D3.2 is stored on this folder. • Monthly meetings (using Teams): consortium meetings have been conducted remotely every month in order to discuss the project progress and address any important issue. All presentations shown in these meetings are stored on this folder. • Task 3.1 - Task 3.6: technical data linked to the experiments/works carried out under the different

	tasks (6 tasks are included in WP3) is stored in the corresponding folders.
Making data findable, including provisions for metadata	The data with regards to the monthly meetings are stored on ASINCAR´s server (WP leader), that has already implemented common high standards about data security and privacy, and in the ALLIANCE SharePoint folder (see previous row). The data are not directly accessible from outside and will not be made available to third parties. Inputs provided concerning the deliverable D3.2 are available through the respective folder on the SharePoint. The dissemination level of deliverable D3.2 will be public and it will be available in the project's website, on the SharePoint folder and in Zenodo. As part of any stored data, metadata will be generated which will include sufficient information with appropriate keywords to help external and internal users to locate data and related information
Making data openly accessible	The datasets generated in each task are not publicly available. All the data are publicly available as part of the aforementioned deliverable D3.2 and through the ALLIANCE website, Sharepoint folder and Zenodo.
Making data interoperable	Outcomes from T2.5 - Interoperability Mechanisms in Complex Food Systems, will provide interoperability mechanisms for data generated in WP3
Increase data re-use	Data are publicly available as part of the aforementioned deliverables and are accessed and re-used by third parties indefinitely without a license.
Allocation of resources	Resources have been allocated according to the project plan and WP3 allocated resources. No additional costs are foreseen for making this dataset FAIR.
Data security	The data are collected for internal use in the project, and not intended for long-term preservation. No personal information will be kept after the end of the project. Furthermore, WISE4 pays special attention to security and respects the privacy and confidentiality of the users' personal data by fully complying with the applicable national, European and international framework, and the

	European Union's General Data Protection Regulation (GDPR) 2016/679.
Ethical aspects	N/A
Other issues	N/A

2.3.1 Task 3.5 - Prevent Food Fraud with Predictive Analytics (INTRA):

Data Summary	Anonymized time-series data from OLYMPOS, stored in the Blockchain provided by UTH, will be used for training deep learning algorithms, and generating predictive analytics. Input data will be numerical and categorical values, whereas trained model's output will be probabilities (a numerical value belongs in the [0,1] interval), integer values (for food fraud risk classes) and string values (food fraud type descriptions). As far as the predictive analytics are concerned, several data will be generated for supporting the creation of several visualizations of interest.
Making data findable, including provisions for metadata	INTRA will keep collected data in an internal database for supporting both training and analytics. Therefore, data will be fully findable in versions. Data and machine learning model versions are expected to be maintained for establishing an effective data value chain.
Making data openly accessible	Especially outcomes obtained from deployed trained deep learning models will be provided to UTH for updating their blockchain and supporting Food Supply Chain traceability.
Making data interoperable	INTRA API for the deployed trained deep learning models' outputs will be in a json format explaining both inputs given to food fraud prevention system and outputs obtained.
Increase data re-use	Yes. Data generated will be used from UTH to support ALLIANCE traceability and of course triggering the generation of several visualizations for a specific observable time window.
Allocation of resources	Project budget is sufficient to cover hosting costs and support ALLIANCE pilots.

Data security	Data will be accessible only from authorized users logging in to the food fraud prevention portal. Predictions will be requested through APIs only from certified users.
Ethical aspects	N/A
Other issues	N/A

2.4 DMP Components in WP4 - Pilot Demonstration and Validation Campaigns (UNIBO)

Data Summary	Data related to WP4 will be stored on WP4 ALLIANCE SharePoint folder and sub-folders. Currently, there are no data or deliverables to collect and store: WP4 activities, in particular T4.1, started in month 12. Other tasks (from T4.2 to 4.8) start their activity in month 20. T4.9 and T4.10 start in month 30.
Making data findable, including provisions for metadata	No data/information has been collected by now in the WP4.
Making data openly accessible	No data/information has been collected by now in the WP4.
Making data interoperable	No data/information has been collected by now in the WP4.
Increase data re-use	No data/information has been collected by now in the WP4.
Allocation of resources	By now, resources have been allocated according to the project plan.
Data security	No data/information has been collected by now in the WP4. The data will be collected for internal use in the project. No personal information will be kept after the end of the project. Privacy and confidentiality of personal data fully comply with the applicable national, European and international framework, and the European Union's General Data Protection Regulation (GDPR) 2016/679. Anonymization of personal data will pursue and respect.

Ethical aspects	N/A
Other issues	N/A

2.5 DMP Components in WP5 - Dissemination, Communication and Exploitation of Results (LC)

Data Summary	Personal details (name, email) of subscribers to ALLIANCE newsletter on Mailchimp The project website is hosted by LC (no personal data) WP5 meetings are held via Teams; minutes and other documents are saved on the project's SharePoint set up by UTH
Making data findable, including provisions for metadata	N/A
Making data openly accessible	WP5 set up a Zenodo community (https://zenodo.org/communities/alliance-againstfoodfraud) to facilitate open access requirements for scientific outputs
Making data interoperable	N/A
Increase data re-use	N/A
Allocation of resources	Project budget (C.3 Other goods, works and services) is sufficient to cover hosting costs.
Data security	Some personal data (newsletter subscribers) are collected for communication and dissemination purposes. Such data will be deleted after the end of the project. Privacy and confidentiality of the users' personal data are respected by fully complying with the applicable

	national, European and international framework, and the European Union's General Data Protection Regulation (GDPR) 2016/679.
Ethical aspects	N/A
Other issues	N/A

2.5.1 Task 5.4 – Marketplace, Systemic Innovations and Industrial Data (INTRA)

Data Summary	Data related to software applications tailored for food fraud detection and predictive analytics will be shared through the ALLIANCE marketplace.
Making data findable, including provisions for metadata	Publicly accessible data describing software applications will be available through the digital platform. Therefore, customers who represent users that are looking to buy software applications from the marketplace will be able to find these data.
Making data openly accessible	Suppliers will have some publicly accessible data about their offerings in the ALLIANCE marketplace, whereas some private information will be shared on a peer-to-peer (P2P) basis.
Making data interoperable	N/A
Increase data re-use	N/A
Allocation of resources	Project budget is sufficient to cover hosting costs.
Data security	Users such as app providers who are looking to provide added-value software applications and suppliers who are looking to sell these applications should be authorized to use ALLIANCE marketplace.
Ethical aspects	N/A
Other issues	N/A

3 FAIR Data Management

ALLIANCE adheres to the FAIR Data Management Principles as recommended by the European Commission, ensuring that data generated by the project remains accessible and reusable for the research community. This adherence covers both public and confidential data and is governed by specific licenses applicable to each dataset.

3.1 Making data findable, including provisions for metadata

To ensure the findability of its data, ALLIANCE uses persistent identifiers (PIDs) such as Digital Object Identifiers (DOIs). These identifiers are crucial as they unambiguously cite and link to the data. Data, along with its rich metadata, is deposited in trusted repositories like Zenodo which facilitates data citation and reuse. The metadata adheres to schemes including Dublin Core, CERIF, and DDI, enhancing the context necessary for data interpretation and enabling automated analysis. Naming conventions for datasets are clearly defined, incorporating elements like dataset status, geographic identifier, institutional affiliation, brief description, project acronym, and a structured version number. This convention ensures consistent updates and version control within Zenodo.

3.2 Making data openly accessible

Aligned with the Open Research Data Pilot, ALLIANCE commits to making research data as openly accessible as possible. The data is documented comprehensively, including clear licensing and provenance details, and is stored securely in compliance with established protocols. Accessibility is facilitated through community-agreed schemas and controlled vocabularies, enhancing the data's integration with other workflows and applications.

Data storage and archiving is 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.

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 licenses)

ALLIANCE aims to increase data reuse through the use of clear licenses that govern the terms of data reuse. The project will use Creative Commons licenses[1], 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.

1 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

In the evolving landscape of food technology and blockchain, ALLIANCE remains steadfast in its commitment to stringent data acquisition, management, and privacy practices. We utilize advanced digital technologies, including sensors and Internet of Things (IoT) devices, to collect and analyse data essential for improving food quality, safety, and tracing consumer behaviours.

ALLIANCE upholds responsible and transparent data collection, ensuring robust measures are in place to maintain privacy and confidentiality of individuals. Our commitment extends to continuously updating our data handling practices to adapt to new technological and regulatory developments.

Utilizing blockchain technology, we aim to revolutionize food supply chain management through secure, transparent, and decentralized record-keeping. This approach significantly enhances traceability, reduces potential fraud, and ensures the highest levels of food safety.

We implement stringent controls to ensure that data is used solely for its intended purpose. This includes obtaining informed consent, adhering to privacy laws, and safeguarding against unauthorized disclosures, particularly sensitive information such as personal data on the blockchain.

Additional Privacy Concerns

Data Accuracy and Integrity: We prioritize maintaining the accuracy and integrity of data, implementing validation processes to protect against data corruption.

Ethical Use of Data: Ethical guidelines govern our automated decision-making processes within the supply chain, ensuring they are just and transparent. These guidelines have been developed internally, drawing upon established industry practices and existing legal frameworks to ensure robust and ethical decision-making throughout the project.

Cross-Border Data Transfers: We address the complexities of global food supply chains by ensuring compliance with international data protection laws, mitigating risks associated with cross-border data transfers.

Consumer Transparency and Consent: Our practices emphasize consumer rights to transparency and consent, ensuring clear communication about the use and benefits of data collection.

Cybersecurity: Given the increased reliance on technology, we continuously enhance our cybersecurity measures to shield our data infrastructure from cyber threats, especially in decentralized networks like blockchain.

Inclusion and Accessibility: We commit to inclusive practices that ensure our technologies are accessible to all users, preventing any form of discrimination or exclusion.

Compliance with Emerging Regulations: Proactively engaging with emerging regulations, we adapt our data management practices to align with new standards and legal requirements, staying ahead of the regulatory curve.

Decentralization Challenges

Despite the benefits, the decentralized nature of blockchain poses unique challenges in controlling personal data. We implement strategic measures to manage these challenges effectively, ensuring both security and transparency without compromising personal data integrity.

As food technology and blockchain technologies continue to evolve, ALLIANCE is dedicated to addressing these and future concerns, enhancing our practices to protect personal information while advancing our technological capabilities. This commitment is vital for building trust and credibility in the industries we serve, ensuring the ethical management of data across all aspects of our operations.

6 Data security

The repository remains our primary platform for publishing and maintaining final project outcomes, deliverables, and scientific publications. Hosted at CERN, it continues to adhere to stringent data security rules as outlined on the Zenodo policies page. We confirm that these practices have been effectively implemented and maintained, ensuring robust protection of our data assets.

The ALLIANCE website and server infrastructure, alongside the ALLIANCE OneDrive, also continue to serve as secure repositories for our project data. Regular security audits have validated the effectiveness of our protective measures, and we have ensured that all data handling complies with the latest data protection regulations.

Our shared folder structure within OneDrive, is actively managed and adapted to meet the evolving needs of the project. Access to this data remains tightly controlled, with encryption, dual-factor authentication, and specific access privileges ensuring that only authorized personnel can access sensitive information.

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 conference calls.
- **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.

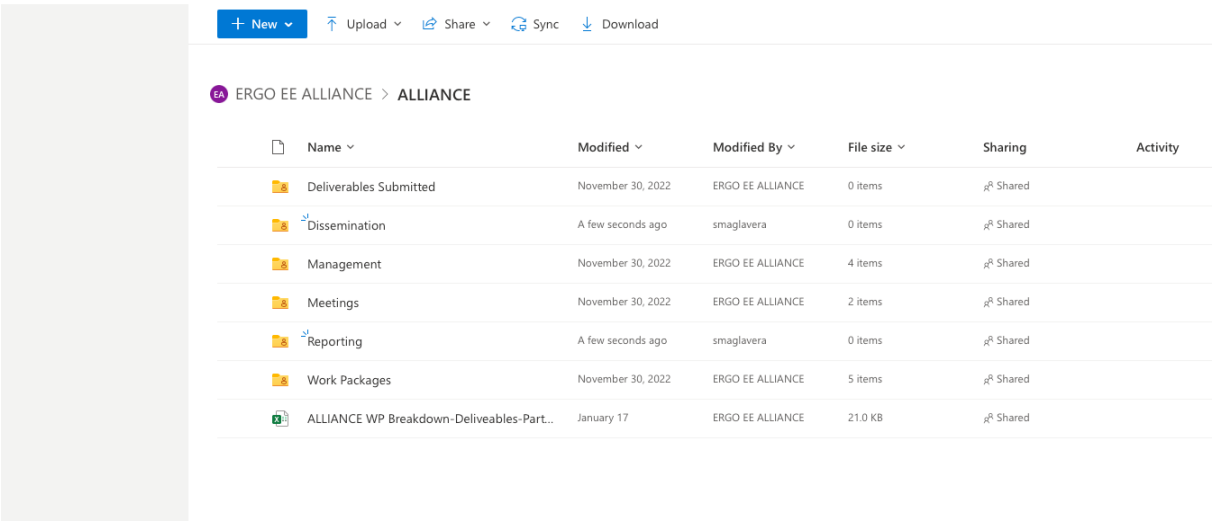

Figure 1- ALLIANCE OneDrive (shared folder)

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 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: The user can modify a file or folder
- Create: The user can create a new folder or file (but not delete it)
- Delete: The user can delete a file or folder

7 Legal and Ethical Aspects

The European Union (EU) has a comprehensive legal framework that governs the use of blockchain technology in the food industry, complemented by key regulations and guidelines:

General Data Protection Regulation (GDPR)[2]: 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[3]: 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[4]: 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[5]: 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[6]: 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.

Introducing the Artificial Intelligence Act

Recently, the EU has taken steps to further secure digital transformations by proposing the Artificial Intelligence Act. This pioneering legislation categorizes AI systems into four risk levels—unacceptable, high, limited, and minimal—mandating strict compliance measures for higher-risk applications. This includes AI systems used in critical infrastructure and sensitive applications that might significantly impact consumer rights or safety. The Act emphasizes risk

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

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

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

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

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

management, data governance, and the necessity for transparency and human oversight in AI operations. Systems posing unacceptable risks, such as real-time biometric identification in public spaces, are prohibited. This Act will significantly influence how AI technologies are deployed within the food industry, ensuring they align with EU standards for safety, transparency, and ethical considerations.

EU-UK Data Adequacy Decision

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.

International Frameworks and Guidelines

Internationally, there is no specific international legal framework for food technology and blockchain. However, some international organizations and initiatives 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.

7.1 ALLIANCE's Compliance

ALLIANCE commits to high standards of ethical practice and compliance with European and international laws. This includes stringent adherence to GDPR for the protection of personal data and proactive engagement with the new requirements under the AI Act. The project employs a robust ethical framework, ensuring all research activities respect personal data and uphold integrity. An ethics committee is in place to address any issues, ensuring continuous alignment with evolving legal standards.

ALLIANCE respects the "do no harm" and "anonymization" principles, especially in AI and blockchain implementations, to protect participant identities and integrity in all data-related processes.

As regulations evolve, such as the introduction of the AI Act, ALLIANCE remains dedicated to staying ahead of compliance requirements, ensuring our practices not only meet current standards but are also poised to adapt to future legislative changes.

The consortium collects 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.

The research is exclusively focused on civil applications and is not expected to lead to risks of misuse, stigmatization of certain societal groups, or 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.

To ensure compliance with research ethics, for ALLIANCE we created a document to log all project activities and assess compliance with research ethics. This document is regularly updated throughout the project to ensure ongoing compliance. The document outlines the ethical considerations of the project and provides guidelines for researchers to follow.

			Main research activities involving human participants						
Research activity (e.g., webinar, workshop, interview, survey, pilot etc.)	Date	Location	Activity leader	Work package/Task	Personal Data (Yes/No)	Other ethical risks	Notes (e.g., provision of consent forms to participants)	Additional information (e.g., number of participants)	Compliant

Figure 2- Research activities involving human participants

7.2 Ongoing Research and Compliance Efforts

As part of our commitment to continuous improvement in ethical standards and legal compliance, ALLIANCE actively engages in ongoing research to explore and address the dynamic landscape of ethics in technology. This is exemplified by our series of insightful blog posts that document our approach and findings:

"Bridging Innovation and Regulation: The AI Act's Role in the ALLIANCE Project"[7]- In this piece, we explore how the AI Act shapes our project's direction and innovation strategies, ensuring that our advancements in AI remain compliant with the EU's emerging regulatory environment.

"Technology Ethics in the Agri-Food Sector: Navigating the Ethical Dimensions Throughout the Innovation Process"[8]- This post delves into the ethical considerations that underpin our work in agri-food technology, detailing how we navigate the ethical landscape throughout the innovation process.

7 https://alliance-heu-project.eu/articles/bridging-innovation-and-regulation-ai-acts-role-alliance-project

8 https://alliance-heu-project.eu/articles/technology-ethics-agri-food-sector-navigating-ethical-dimensions-throughout-innovation

"Championing Ethical AI in the Global Fight Against Food Fraud: The ALLIANCE Project's Pioneering Approach"[9]- Here, we outline our pioneering approach to embed ethical AI practices in our efforts to combat food fraud globally, reflecting our leadership in ethical AI development.

These publications not only highlight ALLIANCE's thought leadership in the area, but also underscore our proactive measures to align our research and operations with the highest ethical and legal standards. Through these discussions, we aim to transparently communicate our strategies and reflections to the wider community, inviting open dialogue and collaboration.

9 https://alliance-heu-project.eu/articles/championing-ethical-ai-global-fight-against-food-fraud-alliance-projects-pioneering

8 Fundamental Rights Consideration

The protection of personal data[10] is a fundamental right as everyone has the right to the protection of their personal data, the freedom of business, and 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.

ALLIANCE continues to recognize and prioritize fundamental rights as enshrined in the Charter of Fundamental Rights of EU. These rights encompass respect for human dignity, freedom of thought, conscience, religion, expression, assembly, equality before the law, and protection against discrimination.

In addition to these established rights, the project also upholds rights that have emerged as particularly pertinent in the context of food technology and blockchain. These include:

Privacy and Data Protection: In line with the GDPR, ALLIANCE ensures the right to privacy through diligent personal data management, only collecting and processing data with full consent and transparency.

Transparency in the Food Supply Chain: The project leverages blockchain to uphold consumers' right to transparency, tracing food from farm to table, and ensuring food safety.

Fair Labor Practices: ALLIANCE advocates for fair labor practices within the food industry, using blockchain to promote transparency and accountability.

Food Security: The project is committed to the right to food security, aiming to make supply chains more efficient, transparent, and sustainable.

While food technology and blockchain are relatively new fields, ALLIANCE proactively applies ethical principles and complies with legal norms in these areas. The emergence of AI has led to additional considerations, which the project addresses by aligning with the EU's AI Act. This act guides us in ensuring that our AI applications, integral to enhancing food technology, are developed and used in compliance with EU values and fundamental rights.

The project maintains a vigilant stance on potential violations of fundamental rights, implementing safeguards and reviewing practices to remain aligned with EU regulations.

ALLIANCE has adopted a proactive approach to integrating ethical, privacy, and data protection principles into every stage of our research and technology deployment. We ensure that these considerations are woven into the project's fabric, from establishing user requirements to the final implementation.

Upholding fundamental rights and societal values is a cornerstone of the ALLIANCE project's success. We will continue to navigate the challenges and opportunities presented by

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

innovative technologies, ensuring that our work contributes positively to society while adhering to ethical and legal standards.

APPENDIX 1

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: The 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 ALLIANCE 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; you must 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 ALLIANCE 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 to 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 ALLIANCE 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 ALLIANCE. 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 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

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 ALLIANCE 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 license 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 interviews, surveys, workshops, webinars, participation in pilots	Personal data might be collected through surveys to be conducted in Task 3.6 - Consumer Demand Assessment and Strengthening	Data will be stored in FBS's cloud repository (Google Drive)
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	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)

		anonymously and in aggregate form	
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 scientist (Dr. Frederic Schedel). 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 accessibility, 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