SecureFood

D1.3 Data Management Plan (v1)

Submission date: 01/07/2024

Due date: 30/06/2024

DOCUMENT SUMMARY INFORMATION

Grant Agreement No	101136583		
Full Title	AN INTEGRATED APPROACH TO ENHANCE FOOD SYSTEMS RESILIENCE, ADVOCATING FOR FOOD SECURITY AND UNINTERRUPTED FOOD SUPPLY		
Start Date	01/01/2024	Duration	42 months
Deliverable	D1.3: Data Management Plan (v1)		
Work Package	WP1 – Project Coordination		
Type	DMP	Dissemination Level	PU
Lead Beneficiary	European Dynamics (ED)		
Authors	Sofia Kordouli, Vassilis Sakas		
Co-authors			
Reviewers	ICCS – Ioannis Kanellopoulos IRIS – Maria del Mar Blanes		

This project has received funding from the European Union's Horizon Europe research and innovation program under Grant Agreement No. 101136583

DOCUMENT HISTORY

Version	Date	Changes	Contributor(s)
V0.1	08/04/2024	Table of contents	ED
V0.2	31/05/2024	Full draft	ED
V0.3	26/06/2024	Internal review	ED
V0.4	01/07/2024	Partner review	ICCS
V0.5	01/07/2024	Partner review	IRIS
V1.0	01/07/2024	Final Version for submission	ED

About SecureFood

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

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

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

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

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

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

PROJECT PARTNERS

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

Table of Contents

LIST OF FIGURES

LIST OF TABLES

List of Abbreviations and Acronyms

Acronym	Meaning
DB	Data Base
DMP	Data Management Plan
DoA	Description of Action
DOI	Digital Object Identifier
DOIs	Digital Object Identifiers
EC	European Commission
ED	European Dynamics
FAIR	Findability, Accessibility, Interoperability, and Reusability
GA	Grant Agreement
IPR	Intellectual Property Rights
WP	Work Package
CoE	Council of Europe

Executive Summary

This deliverable outlines the data management and IPR protection procedures to be followed throughout the SecureFood project and is directly linked and complementary to the D1.2 (Initial Version of Legal, Ethical and Data Management Report). It includes an analysis of the data management policy and the lifecycle for the collected, processed or generated datasets. The plan aligns with the guiding principles of the Horizon Europe Framework Program, emphasizing the essential attributes of findable, accessible, interoperable, and reusable data. These concepts are integrated within the framework of SecureFood's objectives and the specific project requirements.

At the core of this Data Management Plan (DMP) is the comprehensive lifecycle management of data generated and used throughout the project. This encompasses systematic processes for data identification, collection, processing, storage, utilization, sharing, archiving, and eventual disposal. The project's structure and workflow establish a foundation for identifying key data types and sources relevant to the focus of the SecureFood project. The data collection process will be accurately evaluated, and awareness will be raised among all the SecureFood food actors to increase the data quality. The data management plan of T1.3 will monitor data management processes (i.e. for data collection, access and sharing, processing, storage etc.) while the legal and ethical monitoring in T1.5 will address all ethical, legal and privacy aspects related to the project so as to facilitate the data sharing process.

Beyond the traditional data management lifecycle, this DMP addresses unique data requirements, such as handling information related to building operational optimization, food supply chain resilience management systems, and multi-sector interoperability. The plan includes the creation and management of data entries that align with the project's diverse information sources and stakeholders. These entries cover a wide range of information, from digital operational data to interactions within the food supply chain ecosystem.

To manage this data effectively, the DMP introduces a structured management process that includes initialization, assessment, management, and reporting phases. This iterative process is designed to evolve with the project, ensuring that data management practices remain effective and efficient. A key component of this process is a simplified data management template that facilitates consistent documentation of datasets and their lifecycle within the project.

For practical implementation, the DMP proposes an issue tracking tool to assist in maintaining, reporting, and sharing information about the project's datasets. This tool will support data management in line with the DMP's goals and help streamline the associated workflow.

To ensure the DMP's effective operation and integration into the overall project workflow, management actions will focus on raising awareness among project partners. This will be achieved through targeted presentations and workshops focused on data management best practices.

1 Introduction

1.1 Purpose of the Document

This document outlines the initial Data Management Plan (DMP) for the SecureFood project. It provides the foundation for managing data within the project, focusing on establishing core guiding principles for effective data handling. The DMP is designed to assist project members, partners, and practitioners involved in various stages of SecureFood in systematically documenting, managing, and utilizing data. It emphasizes ethical usage and adherence to FAIR principles[1] throughout the project's lifespan and beyond.

1.2 Content and Structure

This section provides an overview of the content and structure of the DMP. The document begins with Section 2, discussing the general guiding principles that form the foundation of the DMP's approach to data management. Section 3 introduces the SecureFood solutions and sets up the DMP framework accordingly. Section 4 explores the data lifecycle and catalogue entry lifecycle, detailing how data will be managed from inception to disposal or archiving. Section 5 covers the principles of FAIR data management, which are central to the project's data handling approach. Section 6 extends the discussion to broader data management considerations, including ethical aspects, data security, and other relevant issues. Section 7 presents the initial data management template and outlines the allocation of resources for data management within the project. Section 8 offers an introduction to the adopted issue tracking and proposed data management workflows. The document concludes with Section 9, summarizing the conclusions drawn so far and outlining future work in data management for SecureFood.

1.3 Intended readership

The intended readership for this deliverable in the SecureFood project includes a diverse range of stakeholders, such as

- Partners and the Project's Advisory Group within the SecureFood project,

- The European Commission (EC),

- Members of the European Union (EU Parliament),

- Other Horizon Europe projects, especially those related to the production, distribution and consumption of food.

- Organizations and experts involved in the SecureFood case studies,

- Other relevant entities, both public and private, including associations representing stakeholders pertinent to the project's scope and objectives.

[1] FAIR Principles: Interpretations and Implementation Considerations published in "Data Intelligence" (2020; 2 (1-2): 10–29), available at https://doi.org/10.1162/dint_r_00024.

1.4 Relationship to other SecureFood deliverables

This document sets the general SecureFood data management plan to be followed throughout the SecureFood project. So, it is an essential document for the SecureFood project and is directly linked to the D1.2 "Initial Version of Ethical, Legal and Data Management Report" (and its' later version D1.6) as well as to the following Data Management Plan Deliverables (D1.4 and D1.5).

2 Guiding Principles

In alignment with the Horizon Europe framework[2], a Data Management Plan (DMP) is essential for effective data management in any research project. For the SecureFood project, the DMP is designed to cover the entire data management lifecycle for all data collected, processed, and/or generated. The goal is to ensure our research data adheres to FAIR principles. To achieve this, the SecureFood DMP will provide detailed information on the following aspects:

- **Data Collection, Processing, and Generation**: Specify the types of data to be collected or generated and the methods of processing. This will include data from various sources in order to have a more comprehensive image including all important parameters that affect the food supply chain.

- **Methodology and Standards**: Outline the methodologies and standards to ensure consistency, quality, and compliance in data handling. This will encompass, as long available, protocols and standard data profiles for data collection, storage, and analysis, as well as standards for data quality and interoperability.

- **Data Sharing and Open Access**: Define the approach to data sharing and open access, including which data will be publicly available, under what conditions, and through which platforms or repositories, ensuring adherence to ethical and legal standards.

- **Data Handling During and After the Project**: Describe the procedures for managing research data both during and after the project. This includes processes for data use, access control, and ongoing management.

- **Data Curation and Preservation**: Detail how data will be curated and preserved over time. This includes strategies for long-term storage, archiving, and ensuring continued access and usability beyond the project's lifespan.

These principles establish a comprehensive data management approach for the SecureFood project, ensuring all data-related activities are conducted ethically, responsibly, and in line with Horizon Europe best practices. Section 4 will elaborate on the project data and catalogue entry lifecycle, while Section 8 will provide further operational details and the full DMP.

2.1 Data Protection Legislative Framework

The SecureFood consortium is highly aware of the ethical implications of its research activities and rigorously adheres to the ethical standards and guidelines set by Horizon Europe and the Charter of Fundamental Rights of the European Union, as stipulated in the Grant Agreement (Article 14 and Annex 5) and D1.3. SecureFood strictly complies with both national and international laws, including:

[2] European Commission (2024). Horizon 2020 Online Manual: Cross cutting issues - Open access & Data management. Online; Retrieved 12-March-2024 from https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, concerning the protection of natural persons in relation to the processing of personal data and the free movement of such data

- The Directive on Privacy and Electronic Communications (2002/58/EC)

- The Directive on Protection of Privacy in the Telecommunication Sector (97/66/EC)

- The Universal Declaration of Human Rights

- The Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Furthermore, SecureFood aligns with Article 19, 'Ethical Principles,' of Regulation No. 1291/2013/EC of the European Parliament and of the Council, which outlines the core ethical principles in research under Horizon Europe. This meticulous approach ensures that all SecureFood activities are conducted with the utmost ethical integrity and respect for fundamental human rights.

3 Initial and Generic Data Items

In line with the SecureFood project's objectives, our data management strategy is founded on the project's core documents, particularly the Grant Agreement (GA). This document offers essential insights into the system architecture and intended use cases for the project, serving as the starting point for identifying and cataloguing the various types of data that the SecureFood project will handle.

The preliminary data outlined in these documents form the nucleus of our data management datasets. These data items are categorized as generic types expected to be generated or utilized across various SecureFood project activities. Each category encompasses a range of data types relevant to developing and demonstrating innovative solutions for the food supply chain.

The data types, their sources, and methodologies for collection and processing constitute the key elements addressed in the SecureFood Data Management Plan (DMP). The comprehensive management of these datasets throughout their lifecycle—from collection and processing to sharing, archiving, and eventual disposal—will be elaborated in subsequent sections of the DMP.

3.1 Data Management Implementation

Table 3.1 serves as a conceptual framework, aligning with the project's core themes. The table is designed to balance the imperative of sharing outcomes publicly while safeguarding sensitive data, reflecting the project's overarching priorities of security, interoperability, and standardization.

Given the project's focus on food supply chain resilience ensuring privacy and data protection is paramount. Hence, employing anonymization and pseudonymization techniques is vital for datasets containing sensitive information, aligning with the project's steadfast dedication to data security and privacy.

In terms of scientific publications, embracing open access is encouraged to amplify impact and broaden dissemination, aligning seamlessly with the project's communication and outreach strategies.

Table 3.1- Data Management Conceptual Framework

Dataset	Classification	Archiving	Safety and Security	FAIR	Privacy & Data Protection
SecureFood Public Deliverables	Public	Every public deliverable is openly accessible on the SecureFood website and will be also stored internally	N/A	Deliverables available on the SecureFood website with metadata	N/A
SecureFood Open-Source Software Components	Public	Source code shared on GitHub or similar repositories	N/A	Source code shared on GitHub or similar repositories	N/A
SecureFood Scientific Publications	Public	SecureFood website and public repositories	N/A	Publications indexed with appropriate metadata	N/A
SecureFood Pilot Data	Public	Near real-time data stored on project DB; Asynchronous and sensitive data stored on premises	Secured under cloud provider or partner's security policies	Data translated to standard models, compliant with FAIR principles for public data. Stored in designated Data Brokers	Anonymization or pseudonimization where applicable
SecureFood Internal Documents	Confidential	Stored in secure internal repositories, access restricted to project members	Access controlled and encrypted storage	N/A	Strict data protection and confidentiality protocols

4 Data and Catalogue Entry Lifecycle

Comprehending the life cycle of data and catalogue entries within the SecureFood project is pivotal for the successful execution of the Data Management Plan (DMP). This life cycle delineates the trajectory of data from its inception through diverse stages of processing, ultimately shaping how it is governed and leveraged within the project.

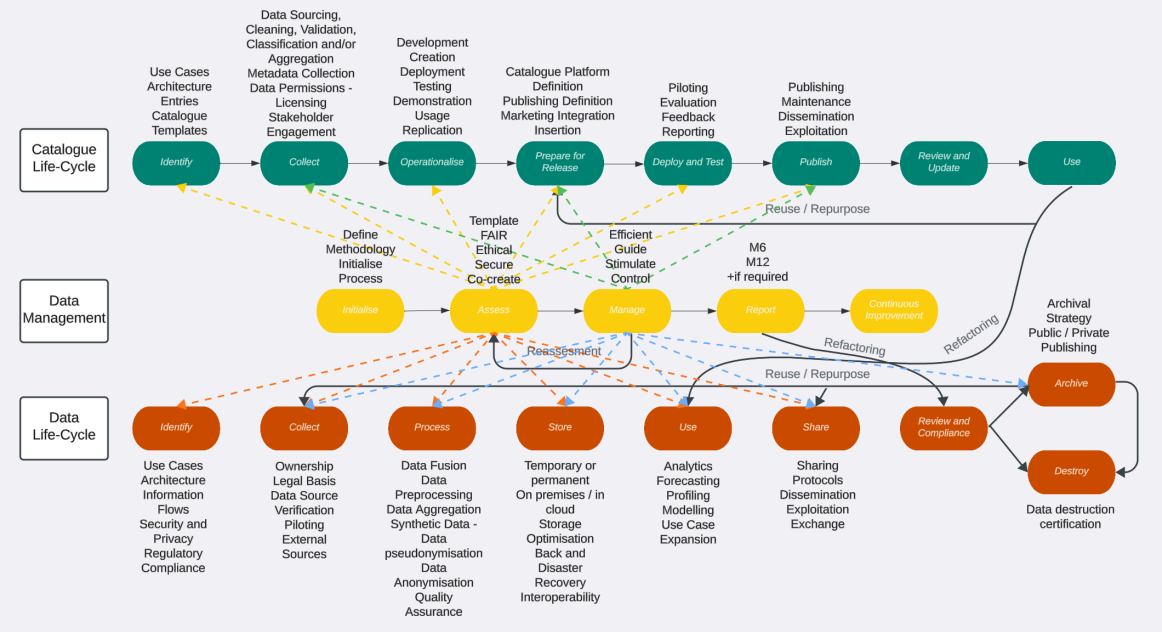

Figure 4.1 - Project Data and Catalogue Life-Cycle and the Data Management process

Dashed arrows denote a more adaptable progression, allowing for flexibility such as the transition from identification to collection. For instance, "Identify" involves understanding what needs to be collected, with actual collection contingent upon factors like resource availability, compliance checks, or stakeholder inputs.

Refactoring arrows denote a feedback loop wherein insights from one step inform improvements in another, fostering continuous evolution of data practices for sustained relevance and effectiveness. This iterative approach also applies to "Reuse/Repurpose" and other arrows.

Figure 4.1 delineates three distinct yet interconnected process flows: Catalogue Lifecycle, Data Management, and Data Lifecycle. Subsequent sections offer concise explanations to orient the reader to the illustration and enhance comprehension of the employed data management processes.

The ensuing content outlines various stages of the processes and includes "GA Reference" sections linking these stages to relevant activities and deliverables outlined in the GA. These reflections contextualize general process steps within the specific scope and objectives of the SecureFood project, demonstrating how each phase of data management and processing contributes to achieving project goals. This approach harmonizes theoretical process steps with practical implementation, showcasing their relevance and integration within the broader framework of the project's objectives and tasks.

4.1 Catalogue Lifecycle

The life cycle of catalogue entries within SecureFood is designed to be dynamic, evolving alongside the project's advancements and technical progress. It stands as a cornerstone of the project's data management strategy, ensuring a systematic and efficient approach to handling the vast array of information generated and utilized. These entries play a pivotal role, encompassing comprehensive details about the solutions and datasets under development.

Closely aligned with the data life cycle, the catalogue entry life cycle is instrumental in planning, executing, and disseminating information both within and beyond the project's scope. The steps involved are as follows:

1. **Identify:** This stage entails defining the catalogue's scope and structure, including use cases, architecture, entries, and templates. It serves as a comprehensive starting point, aligning with deliverables and use cases outlined in various Work Packages (WP), particularly in WP2, which addresses stakeholder requirements and system specifications.

2. **Collect:** This step involves gathering necessary information and utilities for the catalogue through a multifaceted approach. Data sourcing taps into diverse sources, followed by data cleaning and validation to ensure accuracy and relevance. Subsequent steps include data classification, aggregation, metadata collection, and securing data permissions and licensing. Stakeholder engagement seeks feedback to refine the collection process and ensure alignment with user needs and expectations.

3. **Operationalize:** This phase focuses on the practical development, deployment, and testing of the catalogue. It includes development, creation, deployment, testing, demonstration, usage, and replication phases, transforming the catalogue from conceptual design to a functional resource.

4. **Prepare for Release:** This step involves defining the catalogue platform and preparing for publication, ensuring a seamless user experience, access mechanisms, and marketing strategies.

5. **Deploy & Test:** Piloting, evaluation, and feedback collection precede publishing, ensuring the catalogue's readiness for public release and robustness upon launch.

6. **Publish**: Making the catalogue available to the public and maintaining its functionality and relevance over time through maintenance, dissemination, and exploitation activities.

7. **Review & Update:** Allows for iterative improvements based on user feedback, ensuring compliance with regulatory changes and incorporating technological advancements.

8. **Use**: The final step involves external utilization of the catalogue by end-users or stakeholders, contributing to the project's objectives and informing future refinements and developments.

Throughout these stages, reflections from the General Assembly connect specific activities and deliverables to the broader project goals and tasks, ensuring alignment between theoretical process steps and practical implementation within the project's context.

4.2 Data Management

Initialize: This phase marks the inception of the data management process, establishing the methodology and laying the groundwork for subsequent activities. A clear Methodology is defined, outlining protocols, standards, and tools to be employed throughout the data management lifecycle.

Once established, this methodology initiates the data management activities, providing a framework for their execution. This foundational step is pivotal as it sets the parameters within which all future data management tasks will operate. Aligns with WP1, specifically Task 1.3 (Data Management), establishing the groundwork for data management as outlined in Deliverable D1.1.

Assess: This stage involves a comprehensive review of the established Template to ensure its effectiveness in capturing all necessary data attributes and adhering to FAIR principles. Ethical considerations are prioritized, verifying that data management practices uphold the privacy and consent of data subjects. Security protocols are scrutinized to ensure data remains safeguarded against breaches. Additionally, the co-creative processes involved in data development and management are evaluated to ensure meaningful stakeholder collaboration. This phase is instrumental in maintaining a robust and ethically sound data management system, aligned with best practices and continuously refined through stakeholder engagement.

- GA reference: This step mirrors the ongoing assessment in WP8 particularly Task 8.5 (Socioeconomic Impact Assessment and ethical considerations), ensuring alignment with Deliverable D8.8 which focuses on societal impact assessments.

Manage: This phase involves guiding and overseeing data management practices to ensure efficiency and integrity throughout the data lifecycle. Active governance is emphasized, encompassing storage, retrieval, and maintenance of data. Stakeholders are educated on best practices for data usage, fostering innovation and effective application. Control mechanisms are implemented to regulate data access and modifications, ensuring compliance with policies and preserving data integrity. This step is essential for maintaining a high-quality and reliable data management system.

Report: Regular reporting at specified milestones (e.g., M6, M12) ensures ongoing review and updates of data management practices. This step may involve continuous monitoring and reporting rather than fixed milestones, providing documentation and updates on data management practices at key project junctures.

- GA reference: Reflects the structured reporting in WP1, particularly through Deliverable D1.1 (Project Management and Quality Assurance Handbook)

Continuous Improvement: This step embodies the cyclical nature of the data management process, leveraging insights gained from reporting outcomes and evolving project needs to enhance practices continuously. It entails refining methodologies, updating security protocols, enhancing data quality, and ensuring alignment with technological advancements and compliance requirements. This proactive approach fosters growth and adaptation in response to changing regulations, technological innovations, and evolving user needs.

- GA reference: Addresses the iterative improvement approach in WP4 and WP5, that has to do with the design of SecureFood Digital Tools.

4.3 Data Lifecycle

The Data Lifecycle is fundamental to managing data from its inception through its active use to eventual archiving or destruction. It's an ongoing, iterative process that ensures data is handled efficiently and ethically throughout its existence. This aspect of the process is crucial as it encompasses the entire journey of data from its creation to its archival or deletion, ensuring it's treated as a valuable and sensitive asset throughout its lifespan. Each stage is meticulously designed to ensure ethical, legal, and efficient data handling, maximizing its utility while minimizing risks.

Identification: Similar to the Catalogue Lifecycle, this phase involves defining the scope of collected data, including legal and privacy considerations. It's a well-structured process critical for compliance, setting the groundwork for how data will be managed throughout its lifecycle. This phase begins by defining Use Cases to understand specific scenarios in which the data will be used, informing the Architecture to efficiently support these cases. Information Flows are mapped to ensure smooth data transfer, while Security & Privacy measures are integrated from the outset to protect data against unauthorized access and ensure compliance with regulations. Regulatory Compliance is assessed to ensure data handling practices align with current laws, establishing a responsible, secure, and legally sound data lifecycle. This step is vital for establishing data integrity and usability, dictating its value and reliability for future use.

- GA reference: The data lifecycle in SecureFood begins with the crucial phase of data identification, informed by initial project documents, especially the GA, outlining use cases and system architecture. These foundational elements set the stage for identifying the types of data the project will engage with, including use cases derived from various tasks and deliverables across multiple WPs. Legal and ethical considerations, especially regarding personal data, are managed in alignment with WP1 tasks, ensuring GDPR compliance.

Collection: This step lays the ethical and legal groundwork for data collection, ensuring data integrity from collection through its lifecycle. It involves gathering data from various sources while ensuring legality and ownership clarity. Ownership is defined to establish rights and responsibilities over the data, closely tied to Legal basis considerations for GDPR compliance. Data Source Verification ensures the reliability and accuracy of data sources, including validation of data credibility and source reputation. Piloting tests data collection methods on a smaller scale before full implementation, while External Sources may enrich the dataset. This phase ensures data is collected ethically, legally, and securely, establishing a reliable foundation for subsequent processing.

- GA reference: Data collection is guided by specific use cases and system architecture outlined in the GA, relating to tasks and deliverables across WPs such as WP2, WP3, WP4 and WP5. Legal and ethical considerations, particularly regarding personal data, are managed in line with WP1 tasks, ensuring GDPR compliance.

Processing: Data processing steps, including anonymization and pseudonymization, are critical for privacy. This phase transforms collected data into meaningful and secure assets, integrating different datasets through Data Fusion for a comprehensive view. Data Preprocessing refines and cleans data for analysis, while Quality Assurance ensures processed data maintains high standards. This step, integral to various WPs, prepares data for analytics and decision-making tools while ensuring privacy and security.

- GA reference: Data processing, including data cleansing and pseudonymization, is integral to WP4 and WP5, ensuring data preparedness for analytics and decision-making tools while maintaining privacy and security.

Storage: This phase strategically secures processed data, deciding on temporary or permanent storage based on relevance and lifecycle. Choices between on-premises or cloud storage consider factors like accessibility, cost, and security. Storage Optimization maximizes resource efficiency, while Backup & Disaster Recovery plans safeguard against data loss. Interoperability ensures stored data can be used across systems, crucial for maintaining data integrity and availability.

- GA reference: Data storage aligns with requirements laid out in WP2, ensuring data integrity and availability within the SecureFood Middleware architecture.

Usage: This step actively applies stored data to derive value and insights, deciding on temporary or permanent use based on project needs. Analytics interpret data, while Forecasting predicts trends for strategic decision-making. Profiling understands entity characteristics, while Modeling creates simulations. Use Case Expansion explores new data applications, broadening data impact. This phase supports informed decisions and innovations, particularly crucial for WP3 objectives.

- GA reference: Data usage, focusing on analytics for informed decisions, is essential for WP3 and WP5's objectives, which develop Digital Tools for the SecureFood purposes.

Sharing: In this phase, data is distributed beyond its creation and use environments, setting Sharing Protocols for secure, ethical sharing. Dissemination releases data or findings to a wider audience, while Exploitation extracts value for various purposes. Exchange facilitates collaborative opportunities, multiplying data value through wider distribution and use, in alignment with project objectives and dissemination activities.

- GA reference: Controlled data sharing protocols are essential for WP3, WP4 and WP5, ensuring confidentiality. Findings are shared with stakeholders in line with dissemination activities in WP8.

Review and Compliance: This phase ensures data handling, sharing, and usage adhere to established guidelines and policies, with regular compliance checks. It verifies compliance with legal regulations, ethical norms, and organizational policies, identifying discrepancies before data archiving or destruction, ensuring responsible data stewardship and integrity.

- GA reference: This phase aligns with compliance activities outlined in WP1 and monitoring and evaluation in WP6, ensuring data handling adherence to project objectives.

Archive: Data with long-term value is archived, balancing storage costs against potential future value. An Archival Strategy determines how data is stored for future access, considering public or private archives. Publishing ensures data accessibility for ongoing learning and discovery, safeguarding its legacy for future use, in alignment with broader data management objectives and principles.

- GA reference: Archiving strategies are developed in line with data management objectives and principles, ensuring data preservation and accessibility.

Destroy: Finally, data no longer needed or past its retention period is securely destroyed, ensuring privacy and compliance with data protection regulations. Data Destruction Certification provides formal assurance of responsible disposal, preventing potential breaches or unauthorized recovery, aligning with GDPR and ethical guidelines.

- GA reference: Data destruction complies with GDPR and ethical guidelines, ensuring responsible data handling throughout its lifecycle.

5 FAIR Data Management

In the SecureFood project, adhering to FAIR data management principles is essential to ensure that the data collected, processed, and generated are findable, accessible, interoperable, and reusable. These principles, guided by the Horizon Europe framework, are integral to our data management strategies.

Types of Data/Research Outputs

SecureFood is expected to generate and process various types of data. All documents and data will be stored in a way that is easily accessible to both humans and software, as appropriate.

Findability of Data/Research Outputs

Generated data will be traceable and locatable through unique identification mechanisms using standardized naming conventions and file versioning. Additionally, all research data will be annotated with metadata following specific standards, such as the Dublin Core generic metadata[3], to describe the wide range of networked resources.

Accessibility of Data/Research Outputs

Public reports will be shared through public facilities, while confidential reports will be shared within the consortium. Scientific publications will be open access and uploaded to public repositories. Data will be accessible among partners through a common space. Sensitive data related to consumers or users, due to privacy and data protection considerations, will be kept confidential or anonymized before becoming accessible.

Interoperability of Data/Research Outputs

Appropriate standards for data and metadata creation, along with suitable vocabularies, will be developed to ensure interoperability.

Reusability of Data/Research Outputs

Data will be made available as soon as possible and published on the project's website and other repositories. Access will be granted to anyone to use, share, or adapt the data (e.g., remix, transform, or build upon existing material).

Curation and Storage/Preservation Costs

The Project Coordinator will maintain the project document repository, the Scientific Coordinator will be in charge for the quality of scientific data outcomes, and each partner will be responsible for the recoverability of their own generated data.

5.1 Making data findable

In SecureFood, all data management activities—such as storage, processing, and sharing of information among project participants—will be facilitated through a dedicated platform distinct from ProofHub. The project's findings will be shared publicly via the official project website. All data will be archived in the project coordinator's private cloud storage system for a minimum of five (5) years after project completion, with a possible extension of up to two (2) years upon request. Confidentiality, record-keeping, and impact evaluation will follow the same timeline.

[3] www.dublincore.org

A naming convention will be adopted that clearly details the content, data-collecting institution, and publication month. Version control will be applied where necessary, especially when data is withdrawn, with version numbers incorporated into file names.

Technical measures will be implemented to ensure data anonymity, preventing the distribution of identifiable information linked to real names. The project will primarily handle data from various systems related to food supply chain, collected or generated from various sources such as monitoring sensors, smart devices, and user interactions throughout the building management lifecycle.

The data sovereignty module will enhance existing frameworks for data handling and distribution, establishing a data space with open data models, standardized APIs, and effective data sharing policies, all in alignment with FAIR principles.

5.1.1 Data discoverability

Data generated within the scope of SecureFood will be traceable and easily locatable using unique identification protocols. Files will be distinctly identified using standardized naming conventions and file versioning procedures. Metadata annotations will follow standards, such as the Dublin Core generic metadata standard[4], to provide comprehensive descriptions of research data.

To align with FAIR principles, (meta)data will:

- Be associated with a unique and permanent global identifier,

- Include comprehensive metadata for complete data interpretation,

- Be catalogued in a source that facilitates easy searching.

5.1.2 Data Identification Mechanisms

All documents will feature the project's name along with a unique, permanent identifier for the document type and number, as assigned by the coordinator for submission to the European Commission (EC). Each document's identification will also include the relevant task or deliverable number, followed by a concise title of the activity or deliverable. For academic articles, Digital Object Identifiers (DOIs) will be provided by the publisher. Other written works, such as reports and policy recommendations, will receive DOIs through the repository where they are archived, such as Zenodo.

5.1.3 Naming Conventions

To improve data searchability and discoverability, every dataset and deliverable in the project will adhere to a consistent naming protocol and include a version control table. The naming guidelines will ensure

[4] DCMI Usage Board. (2012, June 14). Dublin Core™ Metadata Element Set, Version 1.1: Reference Description. Dublin Core Metadata Initiative. Online; Retrieved 26-March-2024, from https://www.dublincore.org/specifications/dublin-core/dces/

identifiers are meaningful yet concise, avoiding language-specific characters or non-alphanumeric symbols, and appending a two-digit numerical suffix for new document versions.

For deliverables, the naming format will be: Project's name - Dx.y - [Name of the deliverable as described in the DoA], where x represents the work package number and y is the deliverable number within that package. For datasets, the format will be: Project's name - WP [Work Package number] P [Pilot number; pilot activity number] - T [Task number; description of the activity].

The project will employ user-friendly search keywords to facilitate effective data reuse by stakeholders. Keywords will be selected to accurately reflect the dataset content without redundancy and will encompass relevant subjects such as food supply chain resilience, digital Twin Tools, Food Systems etc.

Typically, the keywords will include terms related to the core topics of SecureFood, such as food supply chain, food systems resilience management, early warning mechanism, digital twin technology, etc. Additionally, project-specific keywords, like SecureFood, Horizon Europe, and relevant standards and strategic initiatives, will be used. These keywords will be carefully chosen to ensure relevance and avoid terms that are infrequently used or peripheral to the main content of the project.

5.1.4 Approach towards search keywords

Standardized templates, agreed upon by the consortium, will be used for all documents related to project activities. These templates will feature a designated section for keywords to enhance document findability. This approach ensures that all project-related materials are easily searchable and accessible, supporting the project's commitment to efficient information management and dissemination.

5.2 Open Data Accessibility

Subject to ethical considerations and participant consent, the project aims to maximize data accessibility. SecureFood will employ a secure identity management system, to authenticate and authorize organizations and individuals. Additionally, trusted data exchange mechanisms will ensure not only accessibility but also reliability.

In terms of scientific data production within SecureFood focus areas include:

1. Implementing advanced learning data models to glean deeper insights and facilitate the development of data-driven services for efficient food systems resilience management. These services will leverage rich data from various sources to ensure interoperability with food supply chain stakeholders.

2. Integrating cutting-edge technologies into food supply chain resilience management systems including innovative control, operation, and management methods, to optimize food systems resilience management.

Dissemination strategies for SecureFood reports will vary. Public reports will be shared via public platforms, while confidential reports will be restricted to the consortium. Scientific publications will be freely accessible and uploaded to public repositories. Data sharing among partners will occur through a designated shared space. Some research data, particularly that concerning demo users, will be treated sensitively due to privacy and data protection concerns and will either be handled confidentially or anonymized before being made accessible. While efforts will be made to make data available wherever possible, certain challenges may arise, especially regarding personally identifiable information collected in SecureFood.

5.2.1 Essential methods or software to access the data

Within the SecureFood project, accessing the data won't necessitate any specialized software tools. To ensure both user-friendliness and sustained accessibility, anonymized datasets will be stored in universally accessible formats like Word, PDF, or Excel. This strategy aims to enhance data utilization and accessibility for a diverse user base.

5.2.2 Data deposit, associated metadata, documentation and coding

In SecureFood, each Work Package (WP) leader will be accountable for depositing and safeguarding the data produced within their project tasks. Alongside storage within the WP leaders' systems, duplicates of all final deliverables will be kept on the coordinator's designated project management platform (currently ProofHub) and, for specific maintenance situations, in their cloud storage solution (similar to Dropbox). This two-tier storage strategy guarantees data integrity and accessibility during and after the project's duration.

5.3 Data Interoperability

The principle of interoperability mandates data to be both machine-readable and consistently structured in terminology. In adherence to this principle, the SecureFood project shall utilize open-source, standardized, and domain-agnostic Open APIs to ensure seamless data interoperability across various systems within the food supply chain resilience management domain.

The project will establish protocols for generating data and metadata, alongside developing relevant vocabularies. Achieving data interoperability is crucial for SecureFood, given its focus on crafting data models and ontologies customized for food systems resilience management. Within the project, a significant emphasis will be placed on evaluating and developing standards and interoperable data models, particularly in WP4 and WP5 to facilitate the effortless sharing and integration of data from diverse food supply chain-related systems.

WP4 and WP5 aim to create a fully interoperable, interconnected, and trusted system in alignment with the project's building reference architecture. This involves designing and implementing open service catalogs, app stores, open data space connectors, interoperability middleware, and system integration. The primary focus is on enabling semantic and service interoperability, secure data exchanges, and comprehensive methodologies and digital solutions to support demonstrators' applications.

5.3.1 Data assessment interoperability

In SecureFood, the advanced Data Governance Middleware harmonizes the Function, Information, and Communication Layers in accordance with the creating a flexible framework for its digital platform. Within this framework, partners are responsible for managing data in a format that is both accessible and comprehensive, adapting to the changing needs of stakeholders who may utilize, integrate, or leverage the project's data. Periodic evaluations of data interoperability will be carried out to ensure that the project's data consistently meets the specific requirements of different scenarios, encompassing varied data infrastructures and the distinct objectives or interests guiding data utilization.

5.3.2 Interdisciplinarity and Transdisciplinary

SecureFood is committed to fostering collaboration among experts from diverse disciplines, transcending the confines of traditional academic silos. The project inherently embraces an

interdisciplinary approach, bringing together varied scientific expertise to develop a streamlined, integrated, and intelligent food systems resilience management system. The consortium of partners amalgamates a wide spectrum of capabilities in data generation and processing, harnessing their collective knowledge and proficiency to ensure comprehensive coverage crucial for the successful implementation of all project endeavors.

6 Extended Views

In SecureFood, several expanded perspectives are essential to the data management process, encompassing data security, privacy, ethical considerations, and compliance with various policies and regulations.

Concerning Data Security and Privacy, safeguarding the security and privacy of collected, stored, processed, and utilized data within the project is paramount. The Data Management Plan (v1, v2 and final version), as detailed in Deliverables D1.3, D1.4 and D1.5 addresses the security aspects of data sharing.

Ethical Aspects: The SecureFood project places significant emphasis on ethical considerations, particularly regarding data privacy. Aligned with the project's ethical guidelines and deliverables (T1.5), no personal data is shared outside the project without proper anonymization. Deliverables D1.2 to D1.6, encompassing detailed business models and functional specifications, address ethical concerns inherent in intelligent food supply chain resilience systems to ensure all dimensions are considered in the project's solutions architecture.

Compliance with Policies and Regulations: SecureFood aligns its data management practices with various national, sectoral, company, institutional, or departmental procedures and policies. This alignment ensures compliance across different jurisdictions and organizational contexts, crucial in multinational and multi-institutional collaborations within the project. Specific policies or regulations impacting data management are documented and reported, ensuring transparency and adherence to all applicable guidelines.

These comprehensive perspectives ensure that data management practices are technically sound, ethically responsible, and compliant with relevant standards. Integrated with specific deliverables and tasks, they enhance the overall effectiveness and integrity of data management throughout the project's duration.

7 Data Management Process

The Data Management Process (DMP) in SecureFood synthesizes the information provided in preceding sections. This process comprises several phases:

Initialization: In this initial phase, the methodology for the DMP is established, and the data management process is commenced. The project's inception and the definition of key concepts and processes initiate this phase. The groundwork for this stage is outlined in the deliverable, detailing data management and IPR protection procedures for the project.

Assessment: This phase entails careful monitoring of the data life-cycle stages, utilizing a data management template to document data progression through the life-cycle. The template, outlined in section 7.1, also evaluates adherence to FAIR principles and ethical and security considerations. Project partners most familiar with the data across different pilots where the data originates conduct the assessment. Additionally, the assessment aligns with the development of the catalogue entry life-cycle

and any updates to the entry template. The catalogue is treated as an independent data resource, and its progress is closely monitored.

Management: Central to this phase is the management of the data management process and influence on data life-cycle stages. The process aims for efficiency and guides life-cycle stages, promoting proper assessment and sharing of data. This includes selecting and recommending potential repositories for data publication. Management is facilitated through general and technical meetings, as well as dedicated data workshops.

Reporting: Reporting occurs at scheduled intervals, as described in the D.1.1 "Project Management Handbook" at Month 3, and the final update at the end of the project in Month 42. These updates reflect any significant evolution in data management practices and the inclusion of new data or changes to existing data.

7.1 Data Management Template

The data management template for SecureFood is an elaborated table that expands upon the initial data items introduced in Section 3 of the plan. This extended table incorporates additional fields, including a data identifier, change log, sections for FAIR attributes, Extended views attributes, as well as rows for the dataset owner and its current status, as depicted in the adapted Table 5. Each row of the table corresponds to a distinct dataset relevant to the SecureFood project. This enhancement streamlines comprehensive tracking and management of datasets, ensuring alignment with project objectives and compliance with data management best practices.

Table 7.1 - Data Management Template

Field	Description (Data Set)
Identifier	Unique identifier of the dataset, comprising an abbreviation and version number (e.g., WF-x.y).
Name	The dataset's name
Change Log	A record of changes made to the dataset, including the date of each change and a brief description.
Description	Detailed description of the dataset, akin to that provided in relevant SecureFood deliverables (e.g., D1.6, D4.1)
Type	The dataset's category, as specified in relevant SecureFood deliverables (e.g., D4.1 for design of Food Supply Chain Digital Twin Tools etc.).
FAIR	Conformance to FAIR principles following the project's guidelines, indicated by letters F (Findable), A (Accessible), I (Interoperable), R (Reusable).
Extended	Status regarding extended views, represented by: - S (Security measures applied) - P (Privacy aspects considered) - A (Anonymized if necessary) - E (Ethical considerations) - O (Other relevant issues).
Owner	The dataset's owner or caretaker, typically a partner in the SecureFood project

Status	The dataset's current status, indicating whether it has been shared or not, along with the repository where it is stored (if applicable).
Adaptation	The design of this data management template is intentionally straightforward to simplify the monitoring of datasets assessed in the SecureFood project. It is acknowledged that not all datasets will be suitable for sharing; for those that are shared, the template's information will be expanded to meet the requirements of the target repository. Enhanced dataset information, along with repository details, will be included in an appendix of a subsequent version of this deliverable. This ensures transparency, efficiency, and adaptability of the data management process to the evolving project needs.

7.2 Resources Distribution

Currently, the distribution of resources for data management within the SecureFood project primarily resides in Work Package 1 (WP1). Specifically, one man-month is dedicated to authoring this deliverable. Additionally, all project partners have assigned resources within Task 1.5, which focuses on ethics, exchange requirements specifications, and data management. These resources are designated to contribute to the data management process, encompassing the preparation of deliverables and execution of data management tasks outlined in Section 8 of the Data Management Plan.

In terms of financial aspects, potential costs associated with open access publishing have been integrated into the budgets of certain partners. This proactive measure ensures that any publications arising from the SecureFood project can be freely accessible, augmenting the project's outreach and impact. However, it's important to note that resources for the long-term preservation of data have not yet been specifically addressed or allocated. This aspect necessitates further consideration and planning to ensure the implementation of sustainable and effective long-term data preservation strategies.

8 Data Management Process Implementation Plan

8.1 Data Archiving Implementation

Careful consideration is given to selecting a platform for archiving and preserving our datasets. Choosing a suitable repository involves evaluating several key factors to ensure effective data management and accessibility. These factors include:

- **Assignment of Unique and Persistent Identifiers:** Each dataset receive a unique and persistent identifier. This is crucial for reliable citations, enabling clear tracking of research outputs to specific researchers and contributions from different grants.

- **Creation of Dedicated Dataset Pages with Rich Metadata**: The repository should create individual pages for each dataset, complete with comprehensive metadata. This enhances discoverability, aids in understanding the data, facilitates linkage to publications, and supports proper citation, thus promoting the visibility and reuse of research.

- **Tracking of Dataset Usage:** Features for tracking how data is accessed and downloaded are important. These statistics help in understanding the impact and utilization of the data.

- **Alignment with Community Needs and Trustworthiness:** The chosen repository should not only meet the specific needs of the SecureFood community but also ideally possess a 'trustworthy data repository' certification. This reflects a commitment to the long-term preservation and accessibility of data.

- **Compliance with Specific Data Requirements:** It is important that the repository aligns with specific data management needs, such as accepted data formats, provisions for access, backup and recovery, and service sustainability. Detailed information about these aspects is usually available on the repository's policy pages.

- **Clear Data Citation Guidelines:** The repository should provide clear instructions on how to appropriately cite any data that is deposited.

8.1.1 Proofhub

SecureFood makes use of ProofHub[5], a versatile project management software solution developed by *ProofHub LLC* in 2011, to streamline team collaboration and project coordination. ProofHub is suitable for issue tracking and managing datasets throughout their life cycle. As a browser-based application, ProofHub offers a suite of tools including a task and deadline calendar, file storage spaces, chat functions, and the ability to manage multiple activity streams through distinct topics. ProofHub will facilitate backlog management and the tracking of datasets along with the template information outlined in Section 8.2.

As the project coordinator, EUROPEAN DYNAMICS ADVANCED INFORMATION TECHNOLOGY AND TELECOMMUNICATION SYSTEMS SA (ED) has implemented ProofHub for managing SecureFood's internal project data. Additionally, Dropbox is utilized for internal maintenance and backup purposes. Access to SecureFood's ProofHub system is meticulously managed by ED, ensuring that only authorized partners within the project consortium have access. This approach underscores our commitment to efficient project management and secure data handling, aligning with the collaborative and innovative spirit of the SecureFood initiative.

8.1.2 Zenodo

Zenodo[6] Is built and developed by researchers, to ensure that everyone can join in Open Science.

The OpenAIRE[7] project, in the vanguard of the open access and open data movements in Europe was commissioned by the EC to support their nascent Open Data policy by providing a catch-all repository for EC funded research. CERN, an OpenAIRE partner and pioneer in open source, open access and open data, provided this capability and Zenodo was launched in May 2013.

In support of its research programme CERN has developed tools for Big Data management and extended Digital Library capabilities for Open Data. Through Zenodo these Big Science tools could be effectively shared with the long-tail of research.

Zenodo's capabilities extend beyond the publication of scientific papers and white papers; it also supports the dissemination of structured research data, such as in XML format. An added feature is Zenodo's GitHub connector, which promotes open collaboration on source code and offers version control for diverse data types. All uploaded content is methodically organized using detailed metadata, including contributor names, keywords, date, location, document type, license, and more, with English being the preferred language for textual metadata items. Importantly, all metadata on Zenodo is

[5] https://www.proofhub.com/
[6] https://about.zenodo.org/
[7] https://www.openaire.eu/about

licensed under the Creative Commons 'No Rights Reserved' (CC0)[8] license, ensuring wide accessibility. Notably, uploading results to Zenodo does not alter the ownership or intellectual property rights of the content.

In line with its commitment to open access and data sharing, SecureFood will utilize Zenodo for the long-term storage and dissemination of all public results associated with our scientific publications, ensuring they are readily accessible to the wider research community.

8.1.3 Code Repository (GitHub)

Within the SecureFood project's technical framework, two primary types of repositories are designated for storing the developed programming code. Specific proprietary tools will be stored in private repositories or infrastructures owned by individual project partners. Access to these private repositories will be granted either to all SecureFood consortium members or to selected groups specifically involved with the relevant tools.

For the open-source components of SecureFood the technical team is considering various open-source code repositories, with GitHub being a primary option. GitHub[9] is a highly recognized online platform designed to support the development, management, and version control of distributed source code. It is widely used for managing source code data and encourages global collaboration among developers. GitHub also provides features for documentation and issue tracking.

GitHub's service offerings include both paid and free plans. The free plan allows for an unlimited number of public, open-access repositories with an unrestricted number of collaborators, making it an ideal choice for open-source projects seeking broad dissemination. However, private repositories, which are not publicly accessible, require a paid subscription. GitHub is preferred by many open-source initiatives for its ease of sharing results. It organizes projects and their outputs using metadata like contributor usernames, keywords, timestamps, and file types. According to GitHub's terms of service, the company does not claim any intellectual property rights over the content hosted on its platform. For textual metadata items, English is the preferred language.

8.1.4 SecureFood Platform

The SecureFood platform is designed as a comprehensive ecosystem for managing and integrating diverse datasets, both structured and unstructured, related to Food Supply Chain Resilience Management. This platform aggregates data from various sources, processing it either in batches for services based on aggregate analytics and historical data or via data streaming technologies for near and/or real-time applications. After ingestion, the data undergoes processes for quality enhancement, homogenization, and modeling, enabling efficient sharing with users and transformation into formats suitable for data analytics services. This data is then stored for querying and utilization by food supply chain systems analytics services and platform users.

[8] Creative Commons. CC0. Online; Retrieved [26-March-2024], from https://creativecommons.org/share-your-work/public-domain/cc0/

[9] https://github.com/about

A key component of the platform's data management services is robust security and access control. This system ensures that only authenticated and authorized users and services can access necessary resources, safeguarding user data stored in relational databases. The security framework, detailed in Section 8.4, provides essential features such as data encryption, vulnerability detection and mitigation, and behavior monitoring and auditing of different entities. As SecureFood in its development stages, the specifics of the platform's functionalities are being actively formulated, laying the groundwork for a secure, efficient, and interoperable data management system within the realm of efficient management in food supply chain systems.

8.2 Proposed Workflow for Data Management

ProofHub [10] offers two default workflows: Basic Workflow (which includes two standard work completion stages: To-Do and Done) and KanBan Workflow (which offers three stages: Backlog, In-Process, and Complete). The tool also allows for dynamic management of additional workflows and the creation of custom processes. Since the beginning of the project, an issue tracking workflow comprised of four stages has been used, as illustrated in Figure 8.1:

- **Backlog:** This is where all tasks begin their journey. In this stage, tasks are in a queue, waiting to be actioned. It's a planning and organization phase where tasks are identified and defined but not yet in active progress. This stage is crucial for prioritizing work and ensuring that all necessary tasks are accounted for before the actual work begins.

- **Doing:** Once tasks are moved out of the Backlog, they enter the "Doing" stage. This indicates that work on these tasks has actively started. It's the execution phase where the bulk of the work happens. Tasks in this stage are being worked on by team members, and it's where most of the project's progress is visible. Keeping tasks updated in this stage is vital to provide a clear view of what's currently in progress.

- **Blocked:** This stage is critical for managing impediments and challenges. When a task cannot progress due to an external dependency, lack of resources, or any other blocker, it is moved to the "Blocked" stage. This helps in quickly identifying issues that are hindering progress and need attention. It's essential for efficient project management as it allows teams to address and resolve obstacles promptly.

- **Done:** Tasks that are completed are moved to the "Done" stage. This signifies that the tasks have been accomplished and no further action is required on them. It's a stage for review and closure, providing a clear indication of the project's milestones that have been achieved. It's also useful for retrospective analysis, allowing teams to reflect on completed work, assess the effectiveness of their approaches, and gather insights for future projects.

[10] ProofHub. Manage workflows. ProofHub Help & Support. Online; Retrieved 12-March-2024 from https://help.proofhub.com/plus/tasks/manage-workflows/

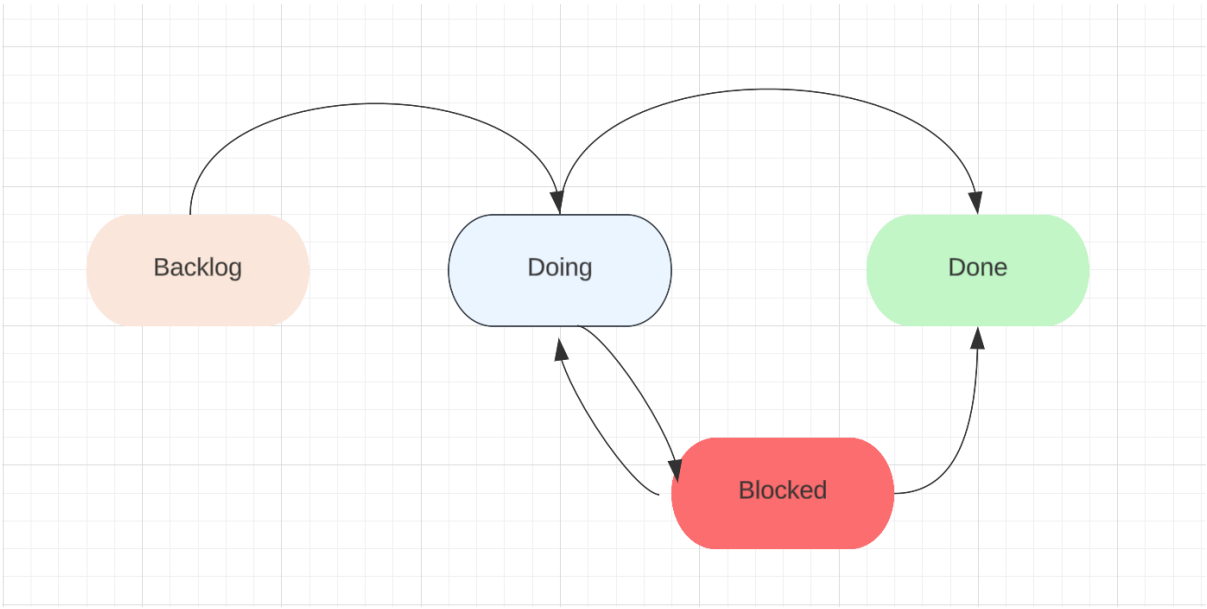

Figure 8.1 - Current Issue Tracking Process Implementation

In the context of SecureFood, this workflow is effectively utilized to manage various tasks, from data collection and processing to ethical reviews and reporting. Each stage of the workflow provides a structured approach to handling different aspects of the project, ensuring clarity, efficiency, and effective progression from task initiation to completion.

Regarding the general content/data management process for SecureFood, the following workflow, as illustrated in Figure 8.2, can be implemented:

- **Open:** This phase involves initializing new datasets within the project. Tasks or items representing these datasets can be created with initial descriptions and relevant metadata. This stage corresponds to the early planning and first steps in data collection and initial assessment.

- **In Progress**: At this stage, the datasets are actively being worked on. ProofHub can be used to track the ongoing processing, storage, and initial usage of the data. Tasks can be updated with progress notes, file attachments, and discussions among team members. This stage aligns with the continuous evaluation and refinement of the datasets.

- **Under Review:** When datasets are ready to be shared or need final approval, they move to the 'Under Review' stage. This can be managed by moving the task to a dedicated list or section for review. Here, datasets are checked for compliance with FAIR principles, ethical considerations, and readiness for external sharing.

- **Published/Rejected:** In this phase, a decision is made on whether the datasets will be published or need to be rejected for specific reasons such as privacy concerns or lack of compliance. Tasks can be tagged as 'Published' or 'Rejected' based on the decision, and notes can be added to provide context for the decision.

- **Report:** The final phase involves documenting and reporting the status of the datasets. This can be handled by generating reports or exporting data that summarize the status and history of each dataset, which can then be included in project reports or updates.

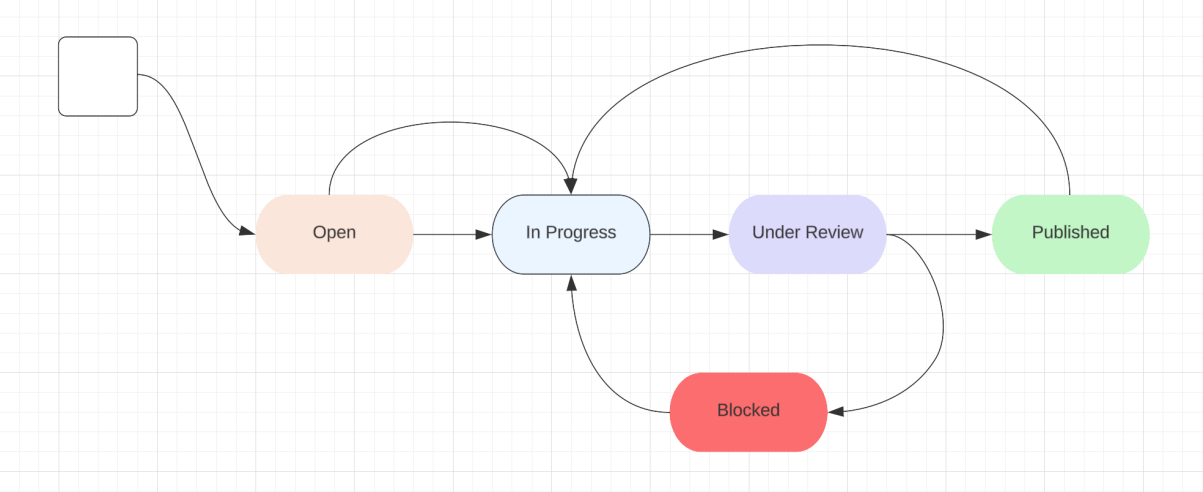

Figure 8.2 - Potential data management process Implementation

Throughout the data management process, ProofHub's features—such as task lists, notes, discussions, and the calendar—are effectively utilized to manage, track, and document the progress and status of each dataset within the project. These features also facilitate communication and coordination among team members involved in the data management process.

8.3 Allocation of Resources

In the context of the SecureFood project, the costs associated with data storage and maintenance post-project completion are expected to be manageable without requiring additional funding. The data generated is anticipated to be highly valuable, particularly given the current and evolving needs of the food supply chain sector and involved stakeholder requirements. While this data is expected to have an immediate impact in the coming years, its relevance may evolve as the sector's challenges and priorities shift.

The **Project Coordinator** is responsible for maintaining the project's document repository. Concurrently, the **Technical Coordinator** ensures the quality of all scientific data outcomes. Each consortium partner in SecureFood is responsible for the recoverability of the data they produce. At this stage, the costs for adhering to the FAIR principles are not yet fully quantifiable, as they will largely depend on the total volume of data generated throughout the project's lifespan.

8.4 Data Security

Task 5.4 focuses on establishing robust data security measures through a comprehensive privacy and cybersecurity framework. This framework ensures the highest levels of security by incorporating detailed access management, anonymization, and encryption for all platform elements. Various security methods are employed, including decentralization, authentication, authorization, auditing, policy-based management, and data encryption. Task 5.4 aims to develop a secure and operational platform by integrating these elements, resulting in a prototype ready for validation.

Additionally, the project ensures data security through the application of established security protocols and frameworks. The data security concept emphasizes the direct involvement of end-users within the

'consumer-centric European data economy,' facilitating mutual benefits for all project participants. The reference architecture, with its focus on interoperability layers, further contributes to a mature, robust, and secure data exchange platform solution.

8.5 Objectives' Ethics, Methodology and Impact

In the SecureFood project, various protocols are implemented to ensure the privacy of participating end-users is safeguarded. The consortium overseeing the project will strictly regulate access to information and enforce necessary restrictions. This is also described in chapter 4.1 and Article 14 (Ethics) of the GA as well as in the D1.2 "Initial Version of Legal, Ethical and Data Management Report". Key measures include:

- Adhering to ethical standards and guidelines in line with Horizon Europe, regardless of the location of demonstrations.
- Providing participants with clear, easily understandable descriptions of the project and study objectives.
- Highlighting the voluntary nature of participation in the project's studies.
- Offering full disclosure on privacy rights and potential impacts on participants' lives, along with details about privacy protection measures such as anonymization and secure data storage.
- Clearly explaining the time commitment and effort required for participation.
- Clarifying the rights of participants to withdraw at any time, including the option to request the destruction of their personal data.
- Making available contact information for project stakeholders.

The consortium will ensure compliance with ethical codes through ongoing reporting processes. In cases of human involvement, participants will be thoroughly informed about privacy, confidentiality, and adherence to national and EU legislation. Clear Information Sheets and Informed Consent Forms detailing the voluntary nature of participation, potential risks and benefits, and procedures for incidental findings will be provided.

Participants will have the opportunity to ask questions and receive comprehensible responses. They may also withdraw themselves and their data at any point without adverse consequences. Signed copies of consent forms will be given to the participant or their legal representative, with originals kept in the participant's research record.

Only anonymized or aggregated data, disconnected from individual identification, will be used for workshops and events. Similar data types will be used for dissemination purposes. If personal data processing is essential under certain conditions, the responsible partner will appoint a Data Protection Officer to oversee GDPR compliance and ensure authorized processing of personal data.

If mandated by European and national legislation, relevant authorities must grant authorization for personal data processing. In cases where platforms like Twitter, LinkedIn, Facebook, or Google Cloud are used, which may involve personal data, a Data Processing Addendum/Agreement will be obtained by the responsible partner.

Lastly, SecureFood's methodology does not involve clinical trials or children's participation. It also does not anticipate environmental damage, stigmatization of specific social groups, adverse political or financial consequences, misuse, or other similar impacts.

8.6 Compliance

The SecureFood consortium acknowledges the significant ethical, fundamental rights, privacy, and data protection concerns that may arise from its project activities. Therefore, it pledges to uphold the highest ethical standards, fundamental rights, and legal compliance, as recognized by the European Union and international organizations. Specifically, the project will align with **essential ethical principles and fundamental rights** (as described in chapter 4.2 of the GA and in SecureFood's D1.2) outlined in various documents, including:

- The Helsinki Declaration Administrative forms[11]
- The European Code of Conduct for Research Integrity (ECCRI, 2011) [12]
- The EU Charter on Fundamental Rights (CFREU, 2010) [13]
- The UNESCO Universal Declaration on Bioethics and Human Rights (2005) [14]
- The European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR, 1950) [15]
- The Universal Declaration of Human Rights (UDHR, 1948) [16]

Regarding privacy and personal data protection, SecureFood will adhere to:

- The General Data Protection Regulation (GDPR) (EU) 2016/679[17]
- The Data Protection Directive (1995/46/EC) [18] and the Directive on Privacy and Electronic Communications (2002/58/EC)[19]
- The EU Charter on Fundamental Rights (articles 7 and 8) (EU 2000/C 364/01)[20]
- The European Convention for the Protection of Human Rights and Fundamental Freedoms (article 8) [21]
- The CoE Convention No. 108 for the Protection of Individuals concerning Automatic Processing of Personal Data (1981)[22]
- The International Covenant on Civil and Political Rights (ICCPR, 1966)[23]

Moreover, the Consortium is prepared for potential changes in the European data protection framework during the project's duration and commits to adhering to any new privacy and data protection regulations. Additionally, it will comply with all relevant national and local regulations applicable to the project's activities.

[11] https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/
[12] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[14] https://www.unesco.org/en/ethics-science-technology/bioethics-and-human-rights
[15] https://www.echr.coe.int/documents/d/echr/convention_ENG
[16] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[17] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[18] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
[19] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058
[20] https://www.europarl.europa.eu/charter/pdf/text_en.pdf
[21] https://70.coe.int/pdf/convention_eng.pdf
[22] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[23] https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

9 Conclusion (and future work)

This deliverable has established the groundwork for the project's data management strategy by creating a comprehensive framework in line with the FAIR (Findable, Accessible, Interoperable, and Reusable) data management principles. It includes a detailed data life cycle tailored to meet the specific needs and objectives of the project, along with a defined data management process that corresponds with the project's diverse and innovative approach.

With the completion of this deliverable, the initial phases of the data management process have been initiated, focusing primarily on assessment and management. To facilitate this process, a sophisticated project management tool, customized to suit the project's requirements, is recommended. This tool will aid in implementing an efficient data management workflow, streamlining the tracking and assessment of datasets. In the upcoming period, the tool will be implemented, and the proposed workflow will be put into operation.

The plan is to introduce this process and tool to the SecureFood project partners, using actual data from the project's pilot studies for demonstration purposes. This hands-on approach will ensure that all partners have a thorough understanding of data management practices and can actively contribute to the project's objectives. Subsequent iterations of this Data Management Plan (DMP) will incorporate ongoing insights and lessons learned from the project, ensuring that data management remains flexible, responsive, and aligned with the project's evolving scope and emerging challenges.