Open-Science and Data Management Plan

D7.4

June 2023

Tools4CAP has received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No. 101086311 . Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

Funded by the European Union

OPEN-SCIENCE AND DATA MANAGEMENT PLAN

Project name	Tools4CAP: Innovative Toolbox empowering effective CAP governance towards EU ambitions
Website	https://www.tools4cap.eu/
Document type	Deliverable
Status	Submitted
Dissemination level	Public
Authors	Bérénice Dupeux and Laura Van den Bossche (ECR)
Work Package Leader	ECR - Ecorys Brussels NV
Project coordinator	ECR - Ecorys Brussels NV

Table of contents

List of Tables

List of Acronyms

CAP	Common Agricultural Policy
CSA	Coordination & Support Action
D	Deliverable
DoA	Description of the Action
DMP	Data Management Plan
DOI	Digital Object Identifier
EU	European Union
FAIR	Findability, Accessibility, Interoperability and Reusability
GA	Grant Agreement
GDPR	General Data Protection Regulation
HE	Horizon Europe
IACS	Integrated Administration and Control System
IT	Information Technology
MS	Microsoft
SP	Strategic Plan
Tools4CAP	Innovative Toolbox empowering effective CAP governance towards EU Ambitions
US	United States
WP	Work Package

1. Executive Summary

This document outlines the data management plan that the Innovative Toolbox empowering effective CAP governance towards EU Ambitions (Tools4CAP) partners are required to follow to achieve the project's objectives. The primary aims of Tools4CAP are to evaluate the application and facilitate the adoption of tools and methods for the design, implementation, and monitoring of the Common Agricultural Policy (CAP) Strategic Plans (SPs). To accomplish this, Tools4CAP will function as a flexible and participatory Coordination & Support Action (CSA) that encourages knowledge designed to boost learning, exchange processes, and the adoption of innovative solutions and good practices. To deliver on these objectives, Tools4CAP will follow a set of core principles to guide the use and management of the project. These principles include:

- Data management will follow the principles of Findability, Accessibility, Interoperability and Reusability (FAIR).
- All data sources used for research within Tools4CAP will be properly referenced, with any restrictions on the use of third-party data identified and is primarily the responsibility of the relevant research teams.
- Any use of data arising from Tools4CAP by third parties should properly acknowledge the origin of the data and respect any restrictions placed on the use of such data.
- Collected data will be made publicly available through an established online repository (e.g. Zenodo) to provide a long-term archive if necessary.
- Data will be identified using an appropriate universal identifier such as a Digital Object Identifier (DOI; www.doi.org/) and accompanied by appropriate and sufficient metadata to make them findable and usable by others.
- Documentation of data will include appropriate metadata, using internationally recognised keywords and identifiers. The relevant task and work package leaders are responsible for their selection.
- Costs related to staff time for providing metadata and archiving data and other outputs will be covered by project partners' resources, as appropriate.
- Data management will follow the best practice by applying reasonable and appropriate technical, physical, ethical and procedural security measures. Attention will be paid to the availability and integrity of data and appropriate levels of authorised access.
- Personal data will be handled in full compliance with the General Data Protection Regulation (GDPR).

2. Introduction

The Tools4CAP Data Management Plan (DMP) describes the strategies and procedures to effectively manage and store project data and deliverables. The plan will contribute to the achievement of the Tools4CAP objectives of thoroughly assessing the application and promoting the uptake of tools and methods used for the design, implementation, and monitoring of the CAP SPs. To this end, Tools4CAP will operate as a flexible and participatory CSA designed to boost learning, exchange processes, and adoption of innovative solutions and good practices. Unlike “Research and Innovation Action” projects under Horizon Europe (HE), which concentrate on direct research activities or technological advancements. Thus, the data used within the project's scope are rarely novel but rather existing data. This data management plan reflects these specificities.

Nevertheless, the data management processes in Tools4CAP will follow the strict guidelines of the GDPR and will adhere to the FAIR principles to improve the findability and usability of the project data and promote its long-term value and impact (Wilkinson *et al*., 2016). In line with the requirements set by HE, the Tools4CAP project will also ensure a secure and reliable data storage environment through a trusted repository. To facilitate the retrievability of the data, it will be provided with a permanent identifier (DOI), so that it can be easily located and accessed by project members and external stakeholders.

Another important aspect of the data management process is the provision of accompanying metadata. This metadata will contain comprehensive information on the characteristics, origin, structure and content of the data. Using standardised metadata, the project aims to facilitate the reusability and contextualisation of the data so that other researchers and stakeholders can understand and effectively use the data and deliverables. Moreover, the use of standardised metadata will greatly improve the efficiency of data retrieval.

Overall, the data management plan for the Tools4CAP project emphasises responsible data management practices, complying with GDPR and embracing FAIR principles. By applying these strategies, the project aims to promote transparency, accessibility, and interoperability, and ultimately maximise the value and impact of the data generated. What follows after this introduction is a data summary which provides a brief overview of the purpose of the data, the types and formats of data to be collected or reused, the origin of the data, and the stakeholder groups that may benefit from the data. Thereafter, each of the FAIR principles is discussed in more detail, followed by the allocation of resources for data management, data security and ethics. Lastly, the annexes provide additional guidance and resources for data management within the project.

3. Data Summary

3.1. Data Purpose

Tools4CAP operates as a flexible and participatory 'Coordination Support Action' to promote learning, exchange processes and adopting innovative solutions and good practices. Therefore, the use and reuse of data in Tools4CAP will – compared to 'Research and Innovation projects' in HE – remain relatively limited and focus mainly on the evaluation of known and novel 'tools' and 'methods' to promote their application for the design, implementation, and monitoring of CAP SPs.

The data in the project is gathered from extensive desk research, an end-user survey, focus groups, case studies and semi-structured interviews in the different Work Packages (WP) to deliver:

- A comprehensive inventory of methods and tools used in the 27 Member States (WP1),
- Methodological guidelines on:
  - Quantitative modelling tools for Ex-Ante and Ex-Post evaluations (WP2),
  - Participatory and multi-governance decision tools (WP3),
  - Novel data and monitoring solutions (WP4)
- A handbook of good practices (WP5)
- A Capacity Building Toolkit (WP6)

Tools4CAP will also utilise a Stakeholder Engagement Platform to boost bottom-up adaptation of innovative methods and tools (WP6). It will establish a Replication Lab to demonstrate their use in 10 Member States and to promote their uptake across the European Union (EU)-27 (WP5). The project will also set up a Capacity Building Hub to help end-users (ministries, management authorities, paying agencies, and other stakeholders) reinforce their capacity to use innovative tools, including models used by the European Commission (WP6).

Moreover, data may be collected and subsequently used to support the implementation of the project's Communication, Dissemination and Exploitation Strategy (WP6, D6.1-D6.4). It will include images, videos, and visualisations to be disseminated through social media channels, such as Twitter and LinkedIn. Materials may be reused for multiple purposes to support different objectives and activities across the project where appropriate and agreed upon.

3.2. Data Types and Format

3.2.1. Data Types and Re(use)

Throughout the Tools4CAP project, publicly available (quantitative and qualitative) data on methods and tools will be reused from existing 'sister' projects (see Annex 1) and relevant grey literature. Reusing this data in Tools4CAP is essential to identify and adapt innovative tools and methods and to build on the experience and expertise of other recent or ongoing research that falls within this project's scope and objectives. These include research that has already made progress in developing Ex-Ante modelling tools for CAP design; Integrated Administration and Control System (IACS), monitoring technologies, and data sources for CAP implementation; and multi-governance and participatory solutions for rural development and policy design. In addition, reusing data reduces duplication and increases the return on existing investments in the models and data created. Building on these data and models, some of their aspects will also be updated during the project, while keeping track of key requirements and dependencies. The existing datasets that are reused in Tools4CAP will also be appropriately acknowledged in reports, papers, and other outputs.

Besides the reuse of data, new data will also be collected through interviews, an end-user survey, focus groups and case studies. An overview of data collection and outputs, by WPs and tasks, is given in Table 1. The details of data collection will be updated at intervals throughout the project period and included in the periodic reports, with any specific information on format, structure, and citation reference, if appropriate.

Table 1. Overview of data collection and outputs in Tools4CAP.

WP & Task	Relevant Deliverable or Milestone	Data collection (input)	Output
WP1 T1.1	D1.1 Inventory of methods & tools used by Member States	Desk research Semi-structured interviews	Publicly available report Online repository on Tools4CAP website Shared through social media and coordination office
WP1 T1.3	D1.3 State-of-the-art evaluation and benchmarking fiches	Desk research End-user survey Focus groups*	10 publicly available benchmarking factsheets to showcase good practices
WP2-4 T2.3, T3.3, T4.3	D2.3, D3.3, D4.3 Methodological guidelines	Desk research Online survey in T3.1 Focus groups* Case studies*	Publicly available methodological guidelines Shared through social media, website + coordination office
WP5 T5.2, T5.3	D5.1-D5.2 Case studies D5.3 Handbook of good practices	10 case studies Focus groups*	Publicly available handbook of good practices Shared through social media, website + coordination office
WP6 T6.2	D6.5, D6.6 Focus groups	2 rounds of focus groups across 16 countries	Publicly available reports
WP6 T6.3	D6.7 Tools4CAP Academy – Capacity building toolkit	10 training modules	Capacity Building Toolkit

* input from focus groups or case studies conducted in other WPs is used for fine-tuning results for this WP

3.2.2. Data Size

Public deliverables, highlights of Tools4CAP events, and scientific publications published by partners will be stored in a community repository called Zenodo[1]. Zenodo is a platform specifically designed for hosting data and publications from EU projects. All other documents will be securely stored in private Microsoft (MS) Teams channels[2]. Both the MS Teams channels and Zenodo community repository have the flexibility to expand in size as needed.

3.3. Data Origins

When using publicly available data from 'sister' projects and grey literature, or when generating new data, the relevant deliverable will provide comprehensive details of data sources. The information will be described and referenced in a specific annex or sub-section. These sections will include the source(s) of the data used, any relevant limitations and ethical considerations associated with the data, and proper citation according to the guidelines stated by the data provider or relevant standards.

[1] Zenodo, https://zenodo.org/

[2] It is often called MS Teams and it is a collaboration platform developed by MS. It provides a unified communication and collaboration hub for teams and organisations, with a range of features and tools to facilitate remote working, team collaboration and communication.

The responsibility for including references to (third-party) data lies with the respective research teams, task leaders, and WP leaders. WP 7 will oversee quality control procedures, which will involve reviewing and verifying the inclusion of any specific requirements regarding the references. Examples of citation are given in Annex 2, following the Interinstitutional style guide of the Publications Office of the EU (2022).

3.4. Data Utility

The outputs and activities of the Tools4CAP project are designed to benefit various stakeholder groups as defined in the Communication, Dissemination and Exploitation strategy (D6.1). These stakeholder groups cover a wide range of actors involved in or interested in the use of tools for the design, implementation, and monitoring of the CAP SPs. They will be reached through various dissemination channels, namely the website & tools inventory, stakeholder engagement platform, Tools4CAP Academy, final conference, external events/scientific journals, consortium networks & channels, public repositories (e.g. Zenodo) and communication channels. A detailed overview of the specific stakeholder groups and types can be found in Table 2 below.

Table 2. Overview of relevant stakeholder groups and types benefitting from Tools4CAP's activities and outputs.

Stakeholder group	Stakeholder type
End users	EU policymakers (notably DG AGRI, DG ENVI, DG CLIMA and JRC), national, regional and local policymakers, managing authorities, or other governmental bodies such as control bodies, paying agencies and delegated bodies, IACS/FADN liability agencies, Local Action Groups
Universities, researchers, and young scientists	Universities, researchers, young scientists, think tanks, educational institutions.
Innovators and developers	Information Technology (IT) and technology development companies, private service providers, advisors, advisory groups and innovator brokers, operational groups
Farmers, producers, and farmers' associations	Cooperatives, farmers unions, interbranch organisations
Other stakeholders relevant to agriculture and rural development	Rural networks, NGOs, CSOs
General audience	Civil society
Other	EU-funded projects, actors related to international trade, food processors

4. FAIR data

4.1. Making Data Findable, including Provisions for Metadata

4.1.1. Persistent Identifiers

A DOI will be assigned to Tools4CAP deliverables and resulting scientific publications to ensure persistent and unique identification. For this purpose, a Tools4CAP community will be created on the Zenodo repository. Public deliverables and scientific publications published by partners will be uploaded to this community and automatically assign DOIs. This approach will ensure that the uploaded content is easily discoverable, allowing researchers, stakeholders, and the wider community to find and reference the Tools4CAP deliverables and scientific publications.

4.1.2. Provisions for Metadata

The effective discovery, use and future accessibility of the project materials for project partners and external stakeholders depend on the provision of metadata. Metadata will be designed to common standards to optimise the visibility and accessibility of project outputs (see examples for metadata standards in Annex 2).

In WP1, an online inventory of different tools will be created and made available through the project website. Each tool will also be provided with metadata, including details of its creator/author/owner, potential end-users, and how and when the tool has been used. A further description and categorisation of these tools can be found in the Inventory of Methods & Tools used by Member States (D1.1).

Overall, metadata has been designed to maximise the discoverability of project materials through direct links and search engines. Ongoing analysis throughout the project will also inform the design and optimisation of the metadata and change in its content requirements may be considered if needed during the course of the project.

4.2. Making Data Accessible

4.2.1. Repository

Project materials will be accessible through two different repositories, providing both public and private access. Firstly, public deliverables and scientific publications published by partners will be available on the project website (coordinated by WP6) and in the Zenodo open repository (coordinated by WP7). Once the materials are approved for online publication by the lead authors and WP leaders, they will be uploaded on the website by WP6 and the responsible party for the deliverable will upload the materials to Zenodo, and link them to the Tools4CAP community. Once uploaded, a DOI will be automatically generated in Zenodo. Subsequently, the repository administrator in WP7 will be responsible for approving the uploaded materials in Zenodo.

Secondly, private channels in MS Teams will serve as a trusted repository for storing the remaining project materials. Access to these private channels will be restricted to project partners and moderated by WP7. The use of MS Teams ensures a secure and collaborative space for sharing information, accessible to all WPs and partners.

4.2.2. (Meta)data

The list of Deliverables in the Description of the Action (DoA – Part A) of the Grant Agreement (GA) provides a summary of the data that needs to be made openly accessible. All deliverables are intended for public access except for the Case Study Set-Up Plans (D5.1), the Communication, Dissemination and Exploitation Strategy (D6.1-6.4) and the Project Planning and Quality Assessment Guidelines (D7.2). These excluded deliverables contain sensitive information and will be kept confidential as per Article 13 of the GA.

To meet the open access requirements, appropriate licences are used, such as the latest available versions of the Creative Commons Attribution International Public License (CC BY) or the Creative Commons Public Domain Dedication (CC 0), or equivalent licences with similar rights. The guiding principle is to be "as open as possible, and as closed as necessary". However, certain circumstances may arise where providing open access to the data would conflict with the legitimate interests of the beneficiary, for example concerning commercial exploitation, or with other constraints, including the EU's competitive interests or the beneficiary's contractual obligations. In such cases, a justification should be provided in this DMP when open access to some or all of the data cannot be provided. Currently, there are no plans for embargos foreseen embargos for the duration of the project.

By adhering to these requirements, the project can promote long-term open access to the deposited data, while considering any applicable restrictions and safeguarding the legitimate interests of the beneficiaries. The open-access materials will be retained for the lifetime of the Zenodo repository.

In addition, it is important to make the metadata of the deposited publications openly accessible under a Creative Common Public Domain Dedication (CC 0) or equivalent and provide information at least about the following:

- Publication (author(s), title, date of publication, publication venue)
- HE or Euratom funding
- Grant project name, acronym, and number

- Licensing terms
- Persistent identifiers for the publication
- Authors (and if possible, their organisations) involved in the action
- Grant

The metadata should also provide comprehensive information on any research outputs or additional software required for reusing or validating the data. This ensures that users have the necessary resources and guidance to make effective use of the data. The metadata will also be accessible for the same duration as its associated data.

If any constraints on accessing the (meta)data arise due to software, data format, or associated with institutional permissions, reasonable attempts will be made to assist prospective users. WP6 will manage and track these issues on the website, while WP7 will handle them in the Zenodo repository. There is no need for a data access committee in Tools4CAP to evaluate or approve access requests to personal/sensitive data.

4.3. Making Data Interoperable

The description of data generated in Tools4CAP follows recognised standards and vocabularies commonly used in libraries. Specifically, the project utilises standards and vocabularies endorsed by the United States (US) Library of Congress (Library of Congress, 2017) through the Linked Data Service and terminology developed by relevant peer groups. By aligning with these established vocabularies, Tools4CAP ensures that the data descriptions are consistent, standardised, and compatible with existing research.

Furthermore, Tools4CAP takes an active approach to ensure a shared understanding and referencing of concepts and topics commonly used within the project. The Tools4CAP Conceptual Framework (D1.2) describes this approach in detail. Tools4CAP promotes consistency and interoperability across data and facilitates effective collaboration among project partners by establishing a common understanding of key concepts, terms, and topics.

To enhance the contextual knowledge and explore relationships between datasets, qualified references will be provided. These references establish connections and linkages between related datasets, enriching the overall understanding of the data landscape. Specifying dependencies and complementarities between data in Tools4CAP will enable users to navigate and explore the data more comprehensively and interconnectedly.

4.4. Increase Data Reuse

Tools4CAP employs various strategies to promote data reuse and maximise the long-term impact of generated materials. A community will be established on the Zenodo repository, providing comprehensive information on research findings, tools, and resources needed to validate conclusions in publications. This central platform will facilitate access to relevant material, encourage data reuse and enable researchers to build on previous findings.

Tools4CAP ensures the immediate availability of deposited publications through the Zenodo repository as part of its open-access policy. Publications will also be made available under the Creative Commons Attribution International Public License (CC BY) or the Creative Commons Public Domain Dedication (CC 0) or an equivalent licence (see also section 4.2.2). This open-access approach encourages the wide use and reuse of results for further analysis, innovation and decision-making. However, specific obligations outlined in the GA must be met before data can be made public. These obligations include protecting the results, maintaining confidentiality, ensuring data security and protecting personal data.

Detailed information on data origin, appropriate citations, and acknowledgement requirements are documented in the relevant deliverables and described in specific annexes or subsections. This will ensure that data users understand its origin and how to properly cite and acknowledge it, thereby promoting consistent and appropriate use of the data in subsequent studies and publications.

Tools4CAP also places a strong emphasis on data quality assurance. Standardised methodological protocols as mentioned in the Project Planning and Quality Assessment Guidelines (D7.2) guarantee consistency and robustness across countries, thereby increasing the reliability and validity of the data. This increases their value for future research and enables meaningful comparisons and analysis between data. The project also addresses ethical aspects of data handling through the Ethics and Gender Guidelines (D7.3).

5. Allocation of Resources

5.1. Responsibilities for Data Management

The responsibility for collecting, analysing and managing scientific data (e.g. semi-structured interviews, end-user surveys, focus groups, and case studies) falls under the relevant beneficiary as identified in the Project Planning and Quality Assessment Guidelines (D7.2). Making materials available through the website is the responsibility of WP6 and through Zenodo repository is managed by WP7 with the support of WP6.

5.2. Estimated Costs

Data collection costs are allocated to each partner to fulfil its commitments to research activities, as specified in the GA. In addition, the main estimated cost relates to the staff time required for preparing appropriate documentation and metadata, uploading it to the repository and providing relevant links to project and institutional websites. It is estimated that, on average, the complete documentation and its verification (e.g. checking content of metadata, spelling, keywords, etc.), will take approximately one person days. These costs are generally negligible when compared to the overall data collection costs.

No other specific costs are expected beyond staff costs associated with making the data available. All data storage costs are included in the budgets of the partners and the relevant WPs, and the use of Zenodo's data repository is free of charge. Additionally, the GA states that for making the data accessible (besides the Zenodo repository), only publication fees in full open-access venues for peer-reviewed scientific publications are also eligible for reimbursement.

5.3. Long-Term Preservation

No specific financial value is expected to be associated with the long-term preservation of the data. However, the long-term storage and preservation of the data generated by the Tools4CAP project will bring several benefits. It will enable comparisons and assessments of changes in evidence on tools and methods over time, facilitating the evaluation of the initial findings on the topic.

The data relating related to the dissemination of the Capacity Building Toolkit (D6.7) and providing an open access tool inventory (D1.1, D1.4 & D1.5) will serve as valuable resources for end-users to leverage the design, implementation, and monitoring of the CAP SPs. These resources will become increasingly important as the demand for tools to assess the effectiveness of policy measures grows.

In addition, certain data within the project may be specific to the unique implementation characteristics of the CAP SP implementation period and not easily reproducible. This could affect the accuracy and validity of subsequent analyses. Therefore, the potential value of long-term data preservation will be particularly evident towards the end of the project, as an essential part of its legacy.

6. Data security

Subject to the levels of confidentiality, integrity and availability, the data will be securely stored and made either publicly or internally accessible in line with relevant legislative, regulatory and contractual requirements. Public information will be accessible and stored on a long-term basis in the Zenodo repository, which is designed to comply with best practices in data security (see Annex 3). Zenodo has user authentication mechanisms in place to control access to user accounts and uploaded content. Users must log in with their credentials and are advised to create 'high strength' unique passwords as best practice. Zenodo complies with relevant data protection regulations, such as the GDPR, and uses appropriate technical and organisational measures to protect user data and respect privacy rights. Incident response procedures are in place to address any security incidents or breaches, supported by monitoring and logging mechanisms to detect and investigate unauthorised access attempts or suspicious activity.

All final outputs will also be securely stored in the MS Teams dedicated to Tools4CAP and backed up to the Ecorys data archive for long-term storage. Internal interim versions of data, deliverables and project information will be

managed using the storage and backup arrangements of the relevant partners and the Tools4CAP MS Teams. Access to the MS Teams channels will be restricted to partners and controlled under the supervision of WP7. Multi-factor authentication will be enabled for user authentication in MS Teams, providing an extra layer of security. Guest accounts that have temporary access to the channels are regularly monitored and reviewed to ensure appropriate access and removed when access is no longer needed (see Annex 3 for further information on security measures in MS Teams). Moreover, internal data management is encouraged to follow best practices on back-up and deletion of data (eg, GDPR (Regulation (EU) No. 2016/679) and "Data Protection and Privacy Ethical Guidelines" (European Commission, 2009)). Data can also be transferred between partners using a secure file transfer site hosted by Ecorys i.e. SharePoint.

Data containing restricted or confidential information (e.g. personal data) will be securely stored and managed in full compliance with GDPR (see also section 7 below).

Lastly, any information security incidents should be reported to the Ecorys IT Service Desk, while personal data breaches can be reported to the Ecorys Data Protection Officer in Brussels. Overall, Ecorys' IT systems and services prioritise the integrity, availability and confidentiality of data to enable efficient management and coordination in projects, like Tools4CAP (see Annex 4 for further information on Ecorys' IT facilities).

7. Ethics

Ethical considerations regarding data in Tools4CAP include the collection and processing of personal data, as described in Article 15 of the GA and in the Ethics and Gender Guidelines (D7.3). Data will be protected in compliance with the Regulation (EU) No. 2016/679 (GDPR), which defines personal data as "any information relating to an identified or identifiable person" (for a full definition, see Article 4[3]).

Within Tools4CAP, personal data will be collected (e.g., name, address, email, CV, phone number) through various methods, such as face-to-face interviews, phone calls, emails, workshops, focus groups, and other events. In line with the GDPR's principle of data minimisation, only necessary and relevant personal data will be collected for the intended purposes, as further detailed in the Ethics and Gender Guidelines (D7.3).

To safeguard the protection of the personal data of all participants, appropriate processes will be implemented in Tools4CAP, including:

- Using pseudonymised and/or anonymised data before it is released to the researcher. This means that any personal information that could potentially identify an individual is removed or hidden.
- Obtaining informed consent from participants through an online consent form in EU Survey and detailed information sheets before data collection and project involvement.
- Ensuring that analysis outcomes should not permit outcomes the re-identification of participants and that results are aggregated spatially or categorically if possible. Researchers will take measures to protect the privacy and confidentiality of individuals.
- Guaranteeing that the use of the data does not cause harm or distress to the participants, and minimising any negative consequences that may arise from the research.

Personal data will be kept for the duration of the Tools4CAP project and the reporting period. If permission is granted to include personal data in project documentation, websites or dissemination materials, it may remain in the public domain. Otherwise, the data will be blocked for use and deleted from storage platforms five years after the end of the project, unless otherwise stated in the updated version of the Open Science and DMP (D7.5).

[3] EU Regulation 2016/679 – Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

8. Conclusions

In summary, the Tools4CAP DMP outlines the comprehensive strategies that will be implemented to ensure effective and responsible management of data throughout the project. The DMP highlights the adherence to recognised standards and vocabularies, the promotion of data reusability and accessibility, the allocation of resources, the implementation of data security measures and compliance with ethical considerations. By following these guidelines, Tools4CAP aims to improve data quality, foster collaboration, facilitate knowledge sharing and contribute to the long-term value and impact of the data generated.

9. References

European Commission*, Data protection and privacy ethical guidelines*, September 2009.

Library of Congress, *Linked Data Service*, 2017, www.loc.gov

Publications Office of the European Union, *Interinstitutional style guide* – , Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2830/215072

Wilkinson, M., Dumontier, M., Aalbersberg, I. *et al*., 'The FAIR Guiding principles for scientific data management and stewardship', *Scientific Data,* 160018, 2016, doi:10.1038/sdata.2016.18.

10. Annexes

10.1. Annex 1: List of Publicly Available Secondary Data

Table 3. Use of publicly available data from relevant 'sister' projects within the objectives of Tools4CAP.

Project name (end-date)	Main results to be used in Tools4CAP [Funding Framework]
FLINT (End date: 2016)	Defined FADN-based Farm Level Indicators for evaluation on CAP cross compliance, sustainability and innovation. [FP7-KBBE]
SENSAGRI (End date: 2019)	Developed innovative prototypes of agricultural monitoring services based on EO Copernicus data. [H2020 – RIA]
SUPREMA (End date: 2020)	Proposes a platform supporting modelling groups linked already through various networks. [H2020 – CSA]
SEN4CAP (End date: 2020)	Sen4CAP provides algorithms, products, and good practices for agriculture monitoring for CAP management [H2020]
PoliRURAL (End date: 2022)	Brings together decision-makers and rural inhabitants to implement advanced policy simulation tools [H2020 – RIA]
NIVA (End date: 2022)	Modernises the CAP by providing digital solutions, e-tools and good practices for e-governance for IACS [H2020 – IA]
SmartAgriHubs (End date: 2022)	Built Digital Innovation Hubs that boost the uptake of digital solutions by the farming sector [H2020 – IA]
MEF4CAP (End date: 2023)	Creates an inventory of future data needs and designs a roadmap for future monitoring [H2020 – CSA]
MINDSTEP (End date: 2023)	Develops and calibrate individual decision-making models for impact assessments [H2020 – RIA]
Ruralisation (End date: 2023)	Analyses trends, and analyses rules, policies and actions to provide access to land [H2020 – RIA]
DESIRA (End date: 2023)	Develops a methodology to assess the impact of digitalisation trends and organise 20 Living Labs [H2020 – RIA]
Sherpa (End date: 2023)	Uses results of research projects to engage stakeholders in 40 Multi-Actor Platforms to inform EU rural policy [H2020 – CSA].
FaST	Develops a platform (based on Copernico and Galileo) to support the CAP [EU-funded]
REECAP	EU-wide informal consortium for the use of economic experimental approaches to evaluate and improve the CAP [EU-funded]
RUSTIK (End date 2026)	Co-designs data-collection approaches and data sources. It co-creates knowledge in 14 regional Living Labs [HE]
GRANULAR (End date: 2026)	Develops indicators and methods to generate novel rural data and populate a repository [HE]
LAMASUS (End date: 2026)	Develops an integrated modelling toolbox for the assessment and monitoring of land-related policies [HE]

10.2. Annex 2: Best Practices for Citations and Metadata

10.2.1. Citation

Following the Interinstitutional style guide of the Publications Office of the EU (2022, 95-96), bibliographic references should be made as follows:

1. Reference to a complete work:
    a. author's surname and initial(s) or first name followed by a comma;
    b. title of the work in italics and, where appropriate, edition number;
    c. publisher, place of publication, year of publication, relevant pages, etc.:

    Example: Butcher, J., *Copy-editing: The Cambridge handbook*, Cambridge University Press, Cambridge, 1975, p. 17
2. Reference to part of a work (contribution or article) or an unpublished paper or mimeograph:
    a. if known, author's surname and initial(s)
    b. title of the article (within quotation marks);
    c. Title of the periodical or the series (in italics);
    d. number, date or frequency;
    e. publisher, place of publication, year of publication:

    Example: 'Economic transformation in Hungary and Poland', *European Economy*, No 43, March 1990, Office for Official Publications of the European Communities, Luxembourg, 1990, pp. 151-167.

    Example: Buigues, P., 'Les enjeux sectoriels du marché intérieur', *Revue d'économie industrielle*, No 45, monthly, Brussels, 1988.

Where an author has two or more publications cited from the same year, it is best to avoid any possible confusion in the references and to make it easier for readers to search for a work in the bibliography. The year of publication should therefore be followed by a lower-case 'a', 'b', 'c', etc., without a space. The reference in the main text takes one of the following forms:

- … according to Xxx [name of author] (2019b), the strategy, developed along five separate axes, has allowed …
- … the strategy, developed along five separate axes (Xxx, 2019b), has allowed …

In this case, the entries in the bibliography have the year in the second position, between brackets, and not in the last or second-last position:

- European Commission (2020a), Biodegradability of Plastics in the Open Environment, Publications Office of the European Union, Luxembourg.
- European Commission (2020b), Compendium of 2019 European Language Label projects, Publications Office of the European Union, Luxembourg.
- European Commission (2020c), Erasmus+ – Annual report 2019, Publications Office of the European Union, Luxembourg.

10.2.2. Metadata

The metadata will be provided for the uploaded Tools4CAP content on the website and in the Zenodo repository. This will describe essential information including the title, date of publication, author(s), keywords, and, in the case of Zenodo, a short description of the document and a persistent identifier. The metadata will also comply with existing specifications, such as the JSON Schema[4] in Zenodo. Moreover, to ensure that the keywords used are relevant and accurate, they will be identified and selected using the US Library of Congress Linked Data Service as a reference. Incorporating these keywords, along with date stamps, into the metadata will improve the discoverability of project materials by facilitating targeted searches by topic and date. Below is an example of the metadata on the website and Zenodo:

Table 4. Example of providing metadata for the Tools4CAP website and Zenodo

Metadata	Website	Zenodo
Title	D7.3 Open-science and data management plan	D7.3 Open-science and data management plan
Author(s)	Bérénice Dupeux Laura Van den Bossche	Bérénice Dupeux Laura Van den Bossche
Date	2023-06-30	2023-06-30
Keywords	Common agricultural policy, Data management, Tools4CAP, Coordination Support Action	Common agricultural policy, Data management, Tools4CAP, Coordination Support Action
Short description	/	The Tools4CAP DMP describes the strategies and procedures to effectively manage and store project data and deliverables. It follows the strict guidelines of the GDPR and will adhere to the FAIR principles to improve the findability and usability of the project data and promote its long-term value and impact. Tools4CAP project will also ensure a secure and reliable data storage environment through a trusted repository. To facilitate the retrievability of the data, it will be provided with a permanent identifier (DOI), so that it can be easily located and accessed by project members and external stakeholders.
Persistent identifier	/	10.5281/zenodo.1234567
Language	Eng	Eng
Resource type	Publication-deliverable	Publication-deliverable
Status	For review	/

Furthermore, **naming conventions** can be used (internally) for deliverables, datasets and other documentation (e.g. administrative, drafts dissemination and related outputs, one-off reports). This is also closely related to approaches to versioning (see further).

The naming convention for final copies of deliverables is:

- Tools4CAP_D<number>_<Deliverable title>

The naming convention for final copies of reports of milestones is:

- Tools4CAP_M<number>_<Milestone title>

The naming convention for final copies of other project reports is:

- Tools4CAP_R<number>_<Report title>

[4] JSON Schema is a specification used in Zenodo to define the structure, format and validation rules for metadata associated with uploaded content. It ensures consistency, validation and easy retrieval of resources in the Zenodo repository.

Reports and other project outputs will be labelled using a multi-level version management system for the **versioning**. The approach follows relevant best practices and guidance (e.g. Stanford University Libraries). This approach will be used for scientific outputs, administrative and management reports, and interim and final reports. The labelling uses a syntax that includes major and minor version characteristics, e.g. 3.1, where the first digit (e.g. 3) represents the major version and the second digit (e.g. 1) represents the minor version. The components are as follows:

- New documents without an existing major version, numbered 0.0.
- Major versions with significant status changes, numbered 1.0, 2.0, 3.0, etc.
- Minor versions based on working edits and changes, numbered 1.1, 1.2, 1.3, etc.

A unique number is assigned to each version of a document, regardless of whether the content is a major or minor version. The Lead Authors working on the relevant WPs determine the significance of the changes made and then assign major and minor version numbers. The Project Management Office identifies the final version by assigning a major version number to a document and renaming the final version for upload and public distribution, following the naming conventions mentioned above.

10.3. Annex 3: Data Security of Zenodo and MS Teams

10.3.1. Zenodo

A full overview of Zenodo's infrastructure (organisational, technical and security) can be found on the following link. The security section is presented below:

- CERN Data Centre: Our data centres are located on CERN premises and all physical access is restricted to a limited number of staff with appropriate training and who have been granted access in line with their professional duties (e.g. Zendo staff do not have physical access to the CERN Data Centre).
- Servers: Our servers are managed according to the CERN Security Baseline for Servers, meaning e.g. remote access to our servers are restricted to Zenodo staff with appropriate training, and the operating system and installed applications are kept updated with the latest security patches via our automatic configuration management system Puppet.
- Network: CERN Security Team runs both host and network-based intrusion detection systems and monitors the traffic flow, pattern and contents into and out of CERN networks in order to detect attacks. All access to zenodo.org happens over HTTPS, except for static documentation pages which are hosted on GitHub Pages.
- Data: Zenodo stores user passwords using strong cryptographic password hashing algorithms (currently PBKDF2+SHA512). Users' access tokens to GitHub and ORCID are stored encrypted and can only be decrypted with the application's secret key.
- Application: We are employing a suite of techniques to protect your session from being stolen by an attacker when you are logged in and run vulnerability scans against the application.
- Staff: CERN staff with access to user data operate under CERN Operational Circular no. 5, meaning among other things that:
- staff should not exchange among themselves information acquired unless it is expressly required for the execution of their duties.
- access to user data must always be consistent with the professional duties and only permitted for resolution of problems, detection of security issues, monitoring of resources and similar.
- staff are liable for damage resulting from any infringement and can have access withdrawn and/or be subject to disciplinary or legal proceedings depending on seriousness of the infringement.

10.3.2. MS Teams

A full overview of the MS team's security measures can be found on the following link. The summary of the security framework for Teams is presented below:

- Teams endorses security ideas like Zero Trust, and principles of Least Privilege access. This section gives an overview of fundamental elements that form a security framework for MS Teams. Core elements are:
- Azure Active Directory (Azure AD), which provides a single trusted back-end repository for user accounts. User profile information is stored in Azure AD through the actions of MS Graph.
- There may be multiple tokens issued which you may see if tracing your network traffic. Including Skype tokens, you might see in traces while looking at chat and audio traffic.
- Transport Layer Security (TLS) encrypts the channel in motion. Authentication takes place using either mutual TLS (MTLS), based on certificates, or using Service-to-Service authentication based on Azure AD.
- Point-to-point audio, video, and application-sharing streams are encrypted, and integrity checked using Secure Real-Time Transport Protocol (SRTP).

- You will see OAuth traffic in your trace, particularly around token exchanges and negotiating permissions while switching between tabs in Teams, for example, to move from Posts to Files. For an example of the OAuth flow for tabs, see this document.
- Teams uses industry-standard protocols for user authentication, wherever possible.

10.4. Annex 4: Ecorys IT facilities

10.4.1. Security

Physical security measures

ECORYS Brussels is situated on the 2nd, 3rd, 6th and 7th floors of a 7-storey building.

Access to our floors is controlled by an access control system, which requires an access card to gain entry. Employees gain access by using their access card, which is a personally registered item. Server equipment is located in the Rotterdam (the Netherlands) office and is only accessible to authorised personnel. For guests, it is standard policy to accompany them to the designated meeting area and back to the exit. Guests are also required to sign in (and out) of our guest register, available at the reception.

There is an alarm system that protects the building outside of office hours.

Logical security measures

ECORYS Brussels uses the ECORYS Netherlands data centre and IT services as outlined below. We make use of Windows 10 laptops and desktops. To log on to the system a username/password combination is necessary. This combination is authenticated against MS Active Directory/Azure Active Directory. The password required is subject to a certain complexity and has to be changed every 40 days.

It is also possible to access the ECORYS network from outside the building. This access is controlled by a two-factor authentication system. To log on, our users go to a website that is SSL encrypted. This website is the front end of our SSL VPN gateway. On this website, they enter a username/password along with the code on their hardware or software token. The code on the token is only valid during the current session and a new code is generated every 30 seconds. Once access has been granted, a desktop management framework is used to manage application access. This application access is based on group membership.

The desktops lock down after 10 minutes of inactivity after which the user's password has to be entered to gain access again.

All of our users have 'standard user' rights, so they are unable to install the software. This helps to protect against spyware and other malware. The servers that facilitate the remote sessions are protected by antivirus and firewall software. Both are centrally managed.

Our operating systems are updated by our Windows Software Update Services (WSUS) server regularly (after testing and approval). Antivirus updates are applied on a daily basis. We also scan all email and web traffic for viruses to prevent the loss of data integrity.

We use encryption on many levels; this includes websites and local storage in different devices (laptop, desktops, tablets, smartphones, etc.). We continuously assess our security measures and the level of encryption to determine if they are still up to standard.

We manage our mobile devices through Mobile Device Management software. Allowing us to remotely wipe devices in case of theft, but also apply security policies to further increase the security of the device.

Datacentre

Our data centre is equipped with a redundant fibre optic network that interconnects our high-specification servers. Also, our offices are equipped with a Gigabit Ethernet Local Area Network. A few examples of our IT services are:

- Directory management;
- Mail services (mailboxes and anti-spam) ;
- File and print services;

- Database management;
- Website development and hosting;
- External DNS management for several ECORYS-owned domain names;
- Firewalls;
- Remote access;
- Etc.

We use the latest industry-standard Dell laptops that run Windows 10. Printing services (colour and mono) are provided using high-capacity networked Xerox printers/copiers. These copiers also have the ability to scan documents to the network. Access to the copiers control panel is managed through personal access cards. Documents submitted for printing as well as scans can only be accessed by the user that submitted the job. We also operate our own reprography facility. Other services include the duplication of CDs and DVDs using copy stations. We have the ability to read in a multitude of data storage devices, like CD/DVD, memory cards, magnetic media and many others. We can also read in all MS Office formats as well as Open Office formats.

Our company has an advanced project management system with integrations into our financial information system. This enables us to handle the billing requirements of this contract with great accuracy. We offer the possibility for website development to support the project as well as special email addresses to accompany the website.

10.4.2. Information handling

Ecorys policy

Ecorys understands the critical importance of data protection and privacy and implements policies towards handling of and access to sensitive information that ensure we meet the highest standards. We have appointed a dedicated privacy policy officer, who oversees these policies for Ecorys Netherlands and the wider Ecorys group. In addition, we have a working group on privacy that continuously reviews our policies and processes, in order to ensure our compliance with the GDPR. Furthermore, we raise awareness of the GDPR within the company through information sessions. We also work with a privacy statement and with data processing agreements when we need to handle personal information provided by clients (or other parties).

Ecorys personnel

Any policy is only as good as the personnel implementing it. With regard to handling sensitive data, only the core project team will have access to the information. This means that analytical and other sensitive tasks will only be conducted by cleared personnel. Colleagues without a security clearance will only handle information for which a clearance is not needed (for example, the translation of the peer review reports will involve only non-restricted information, as this is done by colleagues without a security clearance).

Ecorys technical facilities

Ecorys has an information infrastructure (more information at the beginning of Appendix 2) that prevents unauthorised access to (sensitive) information. This includes measures to control the physical access to the office premises, hardware and documents, as well as measures to control digital access to information. Access is based on authorisation, and all data that needs to be handled in relation to this project shall be saved on a separate hard network location, that is only accessible to the project team members.