RURALITIES - CLIMATE SMART, ECOSYSTEM-ENHANCING AND KNOWLEDGE-BASED RURAL EXPERTISE AND TRAINING CENTRES

D1.1 DATA MANAGEMENT PLAN – INITIAL VERSION

Deliverable D1.1

WP1 – Management

Horizon Europe Grant agreement: 101060876
From 1 October 2022 to 30 September 2027

27/03/2023 by UPM (P6)
Version 2.0

1 DELIVERABLE INFORMATION

Work package	WP 1 – Management
Task	T1.2 Generate the data management plan [M1-M7]
Due date	31.03.2023
Submission date	31.03.2023
Deliverable lead	PEDAL - UPM
Version	2.0
Authors	Ramón Alcarria, Borja Bordel, Tomás Robles (UPM)
Reviewers	Robert Miskuf, Gabor Mester

Keywords	– Climate change mitigation
	– Education, general (including training, pedagogy, didactics)
	– Public sector innovation
	– Rural development studies
	– Training and support
	– Vocational training

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	15/12/2022	Initial document structure	UPM
V0.2	13/01/2023	Review by WP1 leader	PEDAL
V0.3	15/02/2023	Addition of national laws in data protection	Earthwatch
V0.4	27/03/2023	Document final draft	UPM
V1.0	28/03/2023	Final review	PEDAL

Dissemination Level

X	**Public — fully open (automatically posted online)**
	Sensitive — limited under the conditions of the Grant Agreement
	EU classified — RESTREINT-UE/EU-RESTRICTED, CONFIDENTIEL-UE/EU-CONFIDENTIAL, SECRET-UE/EU-SECRET under Decision 2015/444

Disclaimer

Copyright notice

2 TABLE OF CONTENTS

List of figures

Abbreviations and acronyms

Acronym	Description
APIs	Application Programming Interfaces
'AZOP'	Personal Data Protection Agency
BEN	Beneficiary
CCO	Creative Common Public Domain Dedication
CDP	Data Protection Authority
CMS	Content Management System
CODES	Framework for communication, dissemination, exploitation of project results and synergies
COO	Coordinator
DMP	Data Management Plan
DoA	Description of Action
DOI	Digital Object Identifier
DPA	Data Protection Act
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EEA	European Economic Area

EU	European Union
FAIR	Findable, Accessible, Interoperable and Reusable
FOODIE	Farm Oriented Open Data in Europe
GA	Grant Agreement or General Assembly, on depend on the context
GDPR	[General Data Protection Regulation](#)
GDrive	Google Drive
HEP	Horizon Europe Programme
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet Service Provider
ISSN	International Standard Serial Number
KIPER	Knowledge and intellectual property rights
KPI	Key performance indicators
Lean DC	Lean Drive Commons
NDPR	Nigerian Data Protection Regulation
NITDA	National Information Technology Development Agency
OLPPD	Organic Law on the Protection of Personal Data
PII	Publisher Item Identifier
PMO	Project Management Office
POPD	Protection of Personal Data
RURIIS	Ruralities Incubator and Innovation Services
SaaS	Software as a Service
SIMSES	Simplified rural socio-ecological systems
UN	United Nations
URI	Uniform Resource Locator
WP	Work Package
WPL	Work Package Leader
'ZVOP-2'	Slovenian Personal Data Protection Act

3 ABSTRACT

The project 'Climate smart, ecosystem-enhancing and knowledge-based rural expertise and training centers' (Ruralities) delivers an ecosystem-enhancing and climate action driven expertise and learning framework organized in hubs e.g., the 'Ruralities, comprising a series of innovative methodologies with the learner at its core, supported by a comprehensive network of living labs, and a blockchain-based digital platform combining the Internet and wireless technologies, to assist engage, connect and empower actors. This is done via a multi-point approach e.g., multi-actors, multi-disciplines, multi-systems, multi-scale, multi-sectors, and multilevel.

Ruralities is rooted in the recruitment, preparation, training and coaching of 1.000+ facilitators for a variety of tasks (e.g., trainers, facilitators, role models, hub coordinators, etc.), and who play a significant role in creating the matrix and the platform upon which the learning framework is built, develops and evolves. Ruralities proposes to ideate, implement, futureproof, validate and deliver the aforementioned expertise and learning centers via real-scale practicing in 6 simplified rural socio-ecological systems (SIMSES) e.g., demonstrators, 2 in Italy, 1 in the United- Kingdom (UK), 1 in Slovenia, 1 in Spain and 1 in Romania. Ruralities coordinates identified actions of local, regional authorities in supports of rural innovation in regions and economic sectors where rural innovators are not yet engaged in a relevant network.

Ruralities coordinates identified SIMSES networks promoting rural innovation solutions whilst establishing innovative multipoint 'Ruralities Hubs' of expertise and training on rural innovation. This is done via coordinating action for the managing authorities and regional bodies influencing regional and national policy instruments in Italy, the UK, Slovenia, Spain and in Romania.

4 PARTNERS

Number	Role	Short name	Legal name	Country
1	COO	PEDAL	PEDAL CONSULTING SRO	SK
2	BEN	RDRP	ASOCIATIA RURAL DEVELOPMENT RESEARCH PLATFORM	RO
3	BEN	CETRI	CENTER FOR TECHNOLOGY RESEARCH ANDINNOVATION (CETRI) LTD	CY
4	BEN	ASIN	ASOCIACION DE INVESTIGACION DE INDUSTRIAS CARNICAS DEL PRINCIPADO DE ASTURIAS	ES
5	BEN	NIC	KEMIJSKI INSTITUT	SI
6	BEN	UPM	UNIVERSIDAD POLITECNICA DE MADRID	ES
7	BEN	IRI	INSTITUT ZA RAZVOJ I INOVACIJE - IRI	RS
8	BEN	PART	PARTICULA GROUP DRUSTVO S OGRANICENOM ODGOVORNOSCU ZA ISTRAZIVANJE RAZVOJ I PROIZVODNJU	HR
9	BEN	UNIZG	SVEUCILISTE U ZAGREBU AGRONOMSKI FAKULTET	HR
10	BEN	ACTS	AFRICAN CENTRE FOR TECHNOLOGY STUDIES	KE
11	BEN	CITT	CENTRO DE INVESTIGACAO E TRANSFERENCIA DE TECNOLOGIA PARA DESENVOLVIMENTO COMUNITARIO	MZ
12	BEN	EQUIP	EUROPEAN SOCIETY FOR QUALITY AND PATIENT SAFETY IN GENERAL PRACTICE/ FAMILY MEDICINE	DK
13	BEN	MUNI	MUGLA SITKI KOCMAN UNIVERSITY	TR
14	BEN	MARIN	MARIN BIYOTEKNOLOJI URUNLERI VE GIDA SANAYI TICARET LIMITED SIRKETI	TR
15	BEN	ULB	UNIVERSITE LIBRE DE BRUXELLES	BE
16	BEN	INAG	INAGRO, PROVINCIAAL EXTERN VERZELFSTANDIGD AGENTSCHAP IN PRIVAATRECHTELIJKE VORM VZW	BE
17	BEN	AASTMT	ARAB ACADEMY FOR SCIENCE, TECHNOLOGY AND MARITIME TRANSPORT	EG
18	BEN	RRAP	REGIONALNA RAZVOJNA AGENCIJA POSAVJE	SI
19	BEN	YXSAV	YXS AVALANA SRL	RO
20	BEN	UNIVI	UNIVERSITATEA PENTRU STIINTELE VIETII "ION IONESCU DE LA BRAD" DIN IASI	RO
21	BEN	SIRET	ASOCIATIA GRUPUL DE ACTIONE LOCALA SIRET-MOLDOVA	RO

Number	Role	Short name	Legal name	Country
22	BEN	SUA	Sokoine University of Agriculture	TZ
23	BEN	UNINO	UNIVERSITE DE NOUAKCHOTT AL AASRIYA	MR
24	BEN	IFAYA	INSTITUT FACULTAIRE DES SCIENCESAGRONOMIQUES (IFA) DE YANGAMBI	CD
25	BEN	ACD	ALTERNATIVE COMMUNAUTAIRE POUR LE DEVELOPPEMENT DURABLE (ACDD)	CI
26	BEN	PROTO	PROTOTIPI LIMITED	NG
27	BEN	AMVO	ALMANAR VOLUNTARY ORGANIZATION	SD
28	BEN	CDD	COMMUNICATION POUR UN DEVELOPPEMENT DURABLE C.D.D.	TG
29	BEN	YTED	YOUTHS IN TECHNOLOGY AND DEVELOPMENT UGANDA LIMITED	UG
30	BEN	CTIC	FUNDACION CTIC CENTRO TECNOLOGICO PARA EL DESARROLLO EN ASTURIAS DE LAS TECNOLOGIAS DE LA INFORMACION	ES
31	BEN	FHV	FONDAZIONE HOMO VIATOR - SAN TEBALDO	IT
32	BEN	MOFE	MONTEFELTRO SVILUPPO SCARL	IT
33	BEN	MUSE	MUSEUM GRAPHIA	IT
34	BEN	CDM	LA CORTE DELLA MINIERA SRL	IT
35	BEN	DEX	DESARROLLO DE ESTRATEGIAS EXTERIORES SA	ES
36	BEN	REDA	ASOCIACION RED ASTURIANA DE DESARROLLO RURAL	ES
37	BEN	GMV	MONTAGNA VICENTINA SOCIETA COOPERATIVA	IT
38	BEN	MARA	MAROC HORIZON D'AVENTURES	MA
39	BEN	UNWI	UNIVERSITY OF MALAWI	MW
40	BEN	NOMA	0KMNOMADS.ORG	GH
41	BEN	UNIM	MAGYAR AGRAR- ES ELETTUDOMANYI EGYETEM	HU
42	BEN	ENIC	ECOLE NATIONALE D'INGENIEURS DE CARTHAGE	TN
43	BEN	UASZ	UNIVERSITE ASSANE SECK DE ZIGUINCHOR	SN
44	BEN	CPF	CONFEDERATION PAYSANNE DU FASO	BF
45	BEN	UNAD	UNIVERSITY OF RWANDA	RW
46	BEN	ZLAN	ZAMBIA LAND ALLIANCE	ZM
47	BEN	EVRO	EVROSAD PROIZVODNJA TRGOVINA EVETOVANJE D.O.O. KRSKO	SI
48	BEN	SEVO	TURISTICNO DRUSTVO SENOVO	SI

Number	Role	Short name	Legal name	Country
49	BEN	IISAC	ISTITUTO D'ISTRUZIONE SUPERIORE A CECCHI	IT
50	AP	HITP	THE HIGHLANDS AND ISLANDS TRANSPORT PARTNERSHIP	UK
51	AP	ASPI	ASPIRE-IGEN GROUP LIMITED	UK
52	AP	EW	CONSERVATION EDUCATION AND RESEARCH TRUST	UK

5 INTRODUCTION

5.1 Executive summary

The Data Management Plan (DMP) main goal is to cover the data management processes of Ruralities, ensuring an alignment with Horizon Europe FAIR data principles (data must be findable, accessible, interoperable and reusable). The DMP is a living document which will be rereleased three times along the project, updated with the periodic evaluation and assessment and adding level of detail and granularity when processes for data collection are progressing.

The current version D1.1 provides the necessary tools and protocols to manage data collection, access limitations, storage, and publication by following an openly accessible approach, with optimized re-use and interoperability. The DMP, in this way, guides the organization of data and knowledge generated by the project to be useful to other research projects related to rural development and innovation, as well as to interested stakeholders.

5.2 Document structure

This deliverable is structured following the guideline of Horizon programme on FAIR Data Management including the following information:

- Section 5. Introduction of the Data Management Plan and Executive Summary.

- Section 6. Data summary: Description of Ruralities types of data

- Section 7. Description of FAIR DATA characteristics including DMP Review Process & data inventory

- Section 8. Allocation of resources

- Section 9. Data Security

- Section 10. Ethical Aspects and Legal framework, including additional local legislations related to data protection.

- Section 11. Conclusions

At the end of the document some annexes are provided:

- Annex 1 provides the already created tools for data collection with the purpose of elaborating this deliverable.

- Annex 2 describes the Informed Consent Form that will used to request rights to use personal information, during the execution of activities with external stakeholders.

- Annex 3 includes the Privacy Policy for Ruralities official web page.

- Annex 4 contains the Data subject request form, that should be used to submit a request to access or correct information about individuals ("Personal Data").

6 DATA SUMMARY

This section will be dedicated to describe the types of data that will be managed in the Project, how the data collection process will be carried out, and how it relates to the project objectives.

Therefore, in Section 6.1 a classification of the data to be collected in the scope of the Project will be proposed. Section 6.2 will indicate the purpose of data collection, indicating an overview of the characteristics of data required and generated in each task.

6.1 Types of data

Various types of data will be collected in the scope of the project:

- Personal Data: ''any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one of more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person'' .
- Research Data: ''retrospective and prospective clinical, pre-clinical, genetic, longitudinal, follow-up and other information (including but not limited to numerical scores, textual records, images and sounds) about individuals, generated or made available pursuant to the Grant Agreement and/or this Consortium Agreement, and excluding Stakeholder Data'' .
- Stakeholder Data: Referred as information, including but not limited to numerical scores, textual records, images and sounds, about individuals employed by or otherwise linked to a stakeholder and generated or made available by a party pursuant to the project. Also contact person of stakeholders participating in lab events, which can be saved in databases.

These types of data will be reviewed and analyzed in accordance with the data protection legislation of each of the countries participating in Ruralities,

At this moment, it is not possible to identify every possible case that may be faced during the course of the project. Decisions on what activities produce which kind of data can also be made in a deliberative process as and when needed. Final decisions will be made by the respective partner/ WP leader after the issue is discussed with the Coordinator. To facilitate the process, the Coordinator may consult the legal advisors and data management officers. If an agreement is not reach with the relevant partner/ WP leader and the Coordinator, or if deemed necessary, the issue might be taken to the Project Board for a decision.

All updated versions of this deliverable will be shared with and communicated to the Consortium via the SaaS platform and email.

6.2 Purpose of data collection and relation to the objectives of the project

In this project data will be collected to achieve the following objectives:

1. To develop structures with interlinks, based on the following instruments:

    a.   SIMSES
    b.   Pilots
    c.   Etc.

2. To acquire insights into food system trends and related R&I policy frameworks, best practices (showcases) and future R&I breakthroughs;

3. To execute effective and targeted communication and dissemination activities adapted to different stakeholders, as well as develop a plan for continued communication beyond the project, thereby maximizing the outreach and impact of Ruralities outputs and policy recommendations.

4. To carry out scientific studies that yield reports and publications. This is important to contribute to the scientific literature with the experiences and findings of the project. A "Dissemination and Communication Reporting" is currently being prepared by P3 to list the planned scientific articles that will be produced within the project. The publication plan is a living document that will be updated regularly by all partners and its further analysis can generate new ideas and approaches to data management, that will be included in future versions of the DMP. Figure 1 provides a schema of the Dissemination and Communication data collection tool.

			Basic Info			Activity details		Ruralities related	
No. of Action	Partner (ID)	Other partners involved	Date of activity	Place of activity (City, Country or online)	Authors/Contributors	Type of activity (Choose one of the activity categories listed in the drop-down menu)	Title of event, conference, workshop, publication, website article, etc.	Is the activity part of Ruralities?	Role and description of your organisation's involvement (e.g. organiser, facilitator, interviewer, speaker, discussant, author, participant, etc.)

Audience of the event /activity				Material used		
Type o Audience add more lines if 2 or more apply for one entry	Overall No of participants	Gender of Audience (if possible to estimate)	Countries addressed	Type of Ruralities material used add more lines if 2 or more apply for one entry	Quantity of project material used (no. of copies distributed per type of project material)	Link to evidence if applicable, if not, please provide the pdf file

Figure 1. Template of the Dissemination and Communication Reporting plan designed by P3-CETRI

While the focus of the first version of the DMP is mainly on data collected, the next version will also report on data produced in the context of the project and non-sensitive data that can be made publicly available in open data repositories and registered at relevant catalogues.

Considering the description of tasks and deliverables presented in the Grant Agreement, the consortium plans to collect and generate various data sets in the form of publications and other deliverables. A table is specified in DMP to reflect the current status of each task publication plan.

Table 1. Overview of the characteristics of data to be collected in RURALITIES

Tasks	Title	Responsible	Outputs (month, type, diss. level)	Dataset Description & Collection methods	Data utility	Type of data & data format
1.1	Generate the project road map, management action plan and coordinate the project	P1 - PEDAL	D1.6 (M1, Other, SEN)	Minutes from meetings with project partners; minutes and reports from workshops; using Google forms; spreadsheet via consortium	During the implementation phase of the project, data will be collected from management and coordination activities. More specifically, the collection/ generation of data comes up from partners' communication, Quality Assurance processes, progress monitoring, risk analysis, workshops and events.	Captured photographs, written insights, reports presenting outcomes and progress of activities, and participant lists. (.csv, .docx, .xlsx, .pdf, .ppt, .jpeg and .png)
1.2	Generate the data management plan	P6-UPM	D1.1 (M6, DMP, PU). D1.2 (M6, R, PU), D1.4 (M36, DMP, PU), D1.5 (M60, DMP, PU)	Characteristics of data to be collected. GDPR legislation. Google forms; spreadsheet, SaaS platform	Characteristics of data collected serves as a basis for understanding requirements of data storage and data management in the project lifecycle. GDPR legislation collection enables to get insights about barriers and challenges for data exchange among countries.	Survey data per country representative and task leader. .xlsx, pdf.
1.3	Organize the project transnational meetings	P1 - PEDAL		Online survey, spreadsheet via consortium, Google forms.	To prepare, plan, coordinate and ensure the follow-up of each project transnational meeting.	Captured photographs, reports and participant lists. (.csv, .docx, .xlsx, .pdf, .ppt, .jpeg and .png)
1.4	Manage Knowledge and intellectual property rights	P3 - Cetri	D1.3 (M18, R, PU)	Online survey, spreadsheet via consortium, Google forms.	Co-create knowledge management frameworks and a strategy for capacity building activities for knowledge transfer. Structure the project's KIPER framework. Curation of intellectual property. Knowledge management.	.xlsx, pdf, interviews, reports.
2.1	Generate "Ruralities impact action plan"	P12 - Equip	D2.1	Workshop information, utilizing Miro (software) and google docs (software) as information containers.	The purpose is to provide a guiding star for each WP in relation to creating early impact and to establish a reflective practice about improving impact monitoring and assessment. Set up indicators and monitor to guide the activities in the work packages	Interviews, surveys, written text in Miro and Google docs formats.
2.2	Create the work programme topic and destination monitoring framework	P12 - Equip	D2.2	Workshop information, utilizing Miro (software) and google docs (software) as information containers.	The purpose is to provide a guiding star for each WP in relation to creating early impact and to establish a reflective practice about improving impact monitoring and assessment. Set up indicators and monitor to guide the activities in the work packages	Interviews, surveys, written text in Miro and Google docs formats.

Funded by the European Union

Tasks	Title	Responsible	Outputs (month, type, diss. level)	Dataset Description & Collection methods	Data utility	Type of data & data format
2.3	Citizen sensing project monitoring instrument	P7 - IRI	D2.3, D2.7	Some form of text files collected through Google forms	Co-create the Citizen Sensing monitoring framework supported by a mobile app	Word files and Excel files
2.4	Implement multi-layered outcomes impacts integr. and evaluation	P6 - UPM	D2.4, D2.5, D2.6	Development status via Google forms, and spreadsheets. Online surveys to represent showcases.	Elaborate the overall implementation roadmap, propose guidance, equip teams and document planning of activities, events, meetings, report the progress and performance, gather evidence of actions, measures, results and KPIs.	Google forms and spreadsheets. Office 365 formats.
3.1	Ruralities Ethics appraisal scheme	P9-UNIZG	D3.1	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
3.2	Framework for human participation ethics	P1 - PEDAL	D3.2, D3.3	General Data Protection Regulation (GDPR, Regulation (EU) 2016/679);	A detailed consent form on the process, what is collected, how is stored the information, what are the limitations surrounding the use of the information will be co-designed.	csv, .docx, .xlsx, .pdf, .ppt, .jpeg and .png files.
3.3	Framework for personal data collection and process	P49 - IISAC	D3.2, D3.3	General Data Protection Regulation (GDPR, Regulation (EU) 2016/679);	Characteristics of data collected serves as a basis for understanding requirements of data storage and data management in the project lifecycle. GDPR legislation collection enables to get insights about barriers and challenges for data exchange among countries.	Survey data per country representative and task leader. .xlsx, pdf.
3.4	Framework for environment ethics, health and safety	P9-UNIZG	D3.2, D3.3	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
4.1	Create the strategy, identity specific synergies action plan.	P3- CETRI	D4.1, D4.8, D4.9	Names/telephones/ emails of Participants in conferences, various event, webinars. Surveys.	Collection of partner information, logo, images, videos for the website and use in social media accounts. Use it to plan the Communication and Dissemination strategy and raise awareness of the project.	Word files, pdf, excel files, video files. Google forms, Spreadsheets in google docs.
4.2	Implement CODES and continuously augment the project overall visibility	P3 - CETRI	D4.4, D4.10, D4.11, D4.12, D4.14, D4.15	Google analytics from the project's website. Social media analytics (LinkedIn, Facebook, Twitter and Instagram).	The purpose is to monitor the impact of the project to the general public and to various target groups. Furthermore, to show the EC that the project has reached its KPI's and that it has created a great impression.	Data analytics, excel files, word files

Tasks	Title	Responsible	Outputs (month, type, diss. level)	Dataset Description & Collection methods	Data utility	Type of data & data format
4.3	Gamify Ruralities, recruit and equip role model and "replicators"	P14 - ASPI	D4.2, D4.3, D4.7	Office 365 programs (word, presentation, excel, etc) to record collected data. Some video and audio files may also be needed.	Recruit/equip "role models" and "replicators", create a game platform for dissemination purposes. Starting April, we will begin to digitalize the social simulation game (meeting notes, presentations, excel for charting, etc.).	Microsoft Office 365 - Word, Excel, PDF, Databases, Audio/video.
4.4	Generate and implement exploitation of results mechanisms	P9 - UNIZG	D4.6, D4.13,	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
5.1	Engage, connect and empower the actors of the SIMSES	P7 - IRI	D5.1, D5.3, D5.4	Some form of text files collected through Google forms.	Engage, connect, and empower the actors of the SIMSES by defining methodological frameworks and producing documents such as a Memorandum of Understanding	Word files and Excel files
5.2	Cooperate with EU projects, EC and UN services	P9 - UNIZG	D5.2, D5.5, D5.6	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
5.3	Characterise the SIMSES (specific) and national rural landscape (general)	P13-MUNI	D5.6	Documents characterizing project SIMSES. Literature on practices in targeted SIMSES. Value chains. Spreadsheets, and online forms.	Implement a theoretical and conceptual framework for SIMSES characterization. Categorize identified needs/thematic for Ruralities research studies and craft the problems. Characterize the SIMSES landscape and its territorial idiosyncrasies via the aforementioned values chains: demography, ecosystems, biodiversity, configurations, strategies, dynamics and value distribution, interdependencies, resilience and beyond, rural-urban flows, etc.	Word files, Excel files, PDF.
5.4	Characterise the pan-European and pan African Union rural landscape	P8 - PART	D5.6	Minutes, notes, spreadsheet, desk research, online surveys, selection of showcases, Interviews, Records and Documents.	Organize a structured research programme to typify the cross-sectoral and territorial rural innovation landscape. Characterize obstacles to sustainable pathways in identified economic sectors. Benchmark survey and examination of successful use-cases. Gather insight from all policies spheres. Identify challenges to be addressed in the rural areas. Define criteria and requirements for T5.4.	Word files, Excel files, PDF, Audio/Video files (MP3, MP4)
6.1	System thinking methodology	P7 - IRI	D6.1	Text files collected through Google forms as well as some image files such as diagrams	Create a system thinking methodological framework for data gathering and defining relationships between relevant variables	Word files, Excel files, PNG, JPG, JPEG, Adobe files.

Tasks	Title	Responsible	Outputs (month, type, diss. level)	Dataset Description & Collection methods	Data utility	Type of data & data format
6.2	Establish the "Ruralities Co-Labs" living labs network	P9-UNIZG	D6.4, D6.2	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
6.3	Create the "Citizen Rural Sensing" CS monitoring framework	P7 - IRI	D6.5	Some form of text files collected through Google forms.	Create the 'Citizen Rural Sensing' citizen science monitoring framework supported by a mobile app (same one from T2.3 basically).	Word files, Excel files and files related to the app development.
6.4	FAST-TRACT Innovation Management programme	P8 - PART	D6.3, D6.6, D6.7	Minutes, notes, spreadsheet, desk research, online surveys, selection of showcases, Interviews, Records and Documents.	Generate a comprehensive innovation ecosystem with gap analysis. Identify and build accurate services packages to answer identified and assessed needs. Ensure effective co-creative and co-production processes with all actors of the SIMSES. Generate 'Ruralities Incubator and Innovation Services' (RURIIS). Establish the 'Ruralities First Seed' funding scheme.	Word files, Excel files, PDF, PPT, Audio/Video files (MP3, MP4)
7.1	Characterise expertise and establish actionable resources	P9-UNIZG	D7.2, D7.4	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
7.2	Identify and structure innovation projects	P7 - IRI	D7.1	Some form of text files collected through Google forms	Implementing a survey, data analyzing and reporting to generate the Ruralities compendium of projects for rural innovation.	Word, Excel and PDF files
7.3	Practice counselling / guidance to selected initiatives	P7 - IRI	D7.1	Some form of text files collected through Google forms and SIMSES' meetings	Practice counselling and guidance to selected initiatives	Word, Excel and PDF files
7.4	Establish Ruralities expertise center	P9-UNIZG	D7.2, D7.4	Minutes, notes of meetings. Surveys, using Google forms, spreadsheet, SIMSES' meetings, desk research.	Identify challenges to be addressed in the rural areas Create a catalogue of good practices to inspire project partners and external participants. Investigate and understand the evolution of innovation and policy making. Monitor skill developments. Score the performance of EU food systems.	Word files, Excel files, PDF, SQL databases,
8.1	Establish multi-actors onsite and online learning settings	P14 - ASPI	D8.1, D8.2	Office 365 programs to record collected data. Probably video and audio files.	Push training centers, onsite and online learning catalogues. (Audio, Video, Microsoft 365)	Microsoft Office 365 - Word, Excel, PDF, Databases, Audio/video.

Tasks	Title	Responsible	Outputs (month, type, diss. level)	Dataset Description & Collection methods	Data utility	Type of data & data format
8.2	Generate structured learning pathways	P14 - ASPI	D8.3, D8.4	Office 365 programs to record collected data. Probably video and audio files.	Compiling drafted curriculum programme/handbook (Images and Microsoft 365)	Microsoft Office 365 - Word, Excel, PDF, Databases, Audio/video.
8.3	Generate the learning pathways integration and deployment programme	P7 - IRI	D8.5	Office 365 programs to record collected data. Probably video and audio files.	Establish training centers + digital learning platform (See 8.1). Generating the Ruralities scalability plan and a policy framework compendium for deployment	Microsoft Office 365 - Word, Excel, PDF, Databases, Audio/video.
8.4	Establish Ruralities training centres	P7- IRI	D8.6	Some form of text files collected through Google forms	Establishing the RURALITIES interdisciplinary training centers	Word, Excel and PDF files

Funded by the European Union

7 FAIR DATA

Data generated in the project, especially research data should be 'FAIR', that is findable, accessible, interoperable, and re-usable. These principles precede implementation choices and do not necessarily suggest any specific technology, standard, or implementation-solution.

7.1 Making data findable, including provisions for metadata

According to the Ruralities Grant Agreement (Article 17), Metadata of deposited data must be open under a Creative Common Public Domain Dedication (CC 0) or equivalent (to the extent legitimate interests or constraints are safeguarded), in line with the FAIR principles (in particular machine-actionable) and provide information at least about the following: datasets (description, date of deposit, author(s), venue and embargo); Horizon Europe funding; grant project name, acronym and number; licensing terms; persistent identifiers for the dataset, the authors involved in the action, and, if possible, for their organizations and the grant. Where applicable, the metadata must include persistent identifiers for related publications and other research outputs.

All open data, publication and open-source software produced in Ruralities will be identifiable and findable by means of persistent Uniform Resource Locator (URI). If possible and provided that there is support from the institutions participating in Ruralities, results will be assigned a Digital Object Identifier (DOI), so that content is adequately integrated in search engines and in data and scientific repositories.

For data sets not yet released, which include those that are in work in progress, and collaborative ones, two means of publishing this information are established: Ruralities SaaS Platform and Data Repository. These two means are described in detail in Section 7.2.1.

For final data sets, and with the purpose of keeping them permanently available, beyond the duration of the project, the Data Management Plan proposes the use of public repositories:

- For institutions that usually use their own publishing services, the use of institutional repositories will be allowed, as long as they generate permanent URIs for the data. It is also recommended to use repositories that generate DOIs for each published document.

- For institutions that would not have the services to publish data according to FAIR principles, in Ruralities a support mechanism is defined for those cases, using the Zenodo platform[1], which will assign a DOI automatically according to Zenodo's DOI versioning support.

Whether scientific publications will be assigned a unique identifier like DOI, Publisher Item Identifier (PII), International Standard Serial Number (ISSN), etc. depends on the open access strategy (green or gold) chosen by the editors and thus also on the respective scientific publisher and the chosen research repository.

---

[1] https://zenodo.org/

7.2   Making data accessible

7.2.1   Repository

For data sets that include those that are in work in progress, collaborative, and those that belong directly to official outputs (deliverables) of the project tasks, three means of publishing this information are established: Ruralities SaaS Platform, Data Repository, and Official Website:

- Ruralities SaaS Platform: It is the official data repository of Ruralities, based on Google Drive, and allows you to create persistent links for the information. Ruralities SaaS Platform will be used for working documentation (draft deliverables), stakeholder and partner contact information, and working versions of publications.
- Ruralities Data Repository: A repository based on CKAN technology, defined within the framework of WP5, will allow partners to start using the generated data, displaying it in this repository in a more orderly manner, including metadata generation, search functions and spatial visualization. Ruralities Data repository will be used for the publication of datasets, prior to having a version with permanent URIs that can exceed the duration of the project and be maintained in external repositories.
- Official Website[2]: For the final documentation generated within the framework of the project, and directly related to the execution of the project, such as deliverables, and other materials, these elements will be published on the official website of Ruralities.

These three repositories are well-known repositories whose functionality can be trusted. Appropriate arrangements have been explored with these three repositories and there is a permission-based access system, as can be seen in Section 10 Data Security. For the official website and the Ruralities Data Repository, a Privacy Policy is included, as a statement describing how a website collects, uses, and manages users' personal data. The Privacy Policy included in Annex 3 will be used for this purpose.

Additionally, these three repositories ensure that the data or documentation is assigned an identifier. As work in progress data, these repositories, while establishing permanent identifiers, do not resolve the identifier to a digital object. However, as described in the previous section, the consortium makes mechanisms available to partners to publish the data according to FAIR principles, using the Zenodo platform, which will assign a DOI automatically according to Zenodo's DOI versioning support.

7.2.2   Data

The majority of the data will be shared in open-source formats. If the data requires a specific software or service that must be developed to process and decode the information within the dataset, it may be resealed under an open source license (EUPL, Apache, MIT, BSD-3 are suitable options) and made accessible at the end of the project by a GitHub repository, and linked into the same dataset(s) with a specific DOI, so it can be open to reuse in order to process, analyze and decode the datasets. Nevertheless, the license for open data will be selected from the list of licenses conformant with the principles of the Open Definition[3].

Data access is provided through interfaces based on globally adopted standards. For geospatial or domain specific data, this could be e.g. the OGC Web Feature Service for feature data, OGC Web Coverage Service for coverage data, OGC Web Map Service for maps, or the OGC Sensor Observation Service for sensor data. For

---

[2] https://www.ruralities-project.eu/
[3] http://opendefinition.org/licenses

most data access requirements, a standard already exists. For data offline viewing, tools for interpreting, processing and editing of data files downloaded from the data repository, heavily depend on the type and format of the data. Documentation of (open source) software needed to access the data will be compiled and developed by Ruralities partners and included in the appropriate deliverables.

7.2.2.1 Data restrictions

Some datasets generated by SIMSES might be stored in databases which are not available through the Open Data portals. Once the use case specification and requirements have been completed this data may also be needed for the processing and visualization in Ruralities domain. However, this data – in its raw format – may not be made available to external stakeholders for further use due to licensing and/or privacy issues. In that case, the data management plan will not cover these datasets.

In case of Commercial Exploitation of a dataset, a registration procedure for all those interested in such datasets will be implemented. This includes the opportunity, to differ the conditions for access depending on type of the inquirer or planned re-usage (e. g. dataset is free of charge for public scientific institutions for scientific work, but with a charge in case of commercial re-use by a company). After registration of the request of a dataset, a time limited download link will be provided via e-mail to the registered contact together with the terms of usage and invoicing procedure. The requisition will be implemented in the metadata, which are available free of charge in any case, in the category "Access".

7.2.3 Metadata

According to the Grant Agreement (Article 17, Open Science), Metadata of deposited data must be open under a Creative Common Public Domain Dedication (CC 0) or equivalent (to the extent legitimate interests or constraints are safeguarded), in line with the FAIR principles (in particular machine-actionable) and provide information at least about the following: datasets (description, date of deposit, author(s), venue and embargo); Horizon Europe or Euratom funding; grant project name, acronym and number; licensing terms; persistent identifiers for the dataset, the authors involved in the action, and, if possible, for their organizations and the grant. Where applicable, the metadata must include persistent identifiers for related publications and other research outputs.

Metadata management will be done according to OpenAIRE Guidelines[4], which helps repository managers expose publications, datasets and CRIS metadata via the OAI-PMH protocol in order to integrate with OpenAIRE infrastructure.

The default metadata repository for final datasets and publications is Zenodo (http://www.zenodo.org). Zenodo is an EC-co-funded, multidisciplinary repository, for publications and data. A DOI is automatically assigned to all Zenodo files, which can be uploaded in any file format. Zenodo allows researchers to deposit both publications and research data, while providing means to link them. Data is stored in the CERN cloud infrastructure, which guarantees that metadata will remain available, even if other domains are no longer available. Zenodo is compliant with the open data requirements of Horizon Europe, the EU Research and Innovation funding programme and OpenAIRE. Furthermore, a Ruralities project page (community) has been set up[5] for easy upload of project datasets y scientific publications. Figure 2 shows the created Ruralities Community in Zenodo.
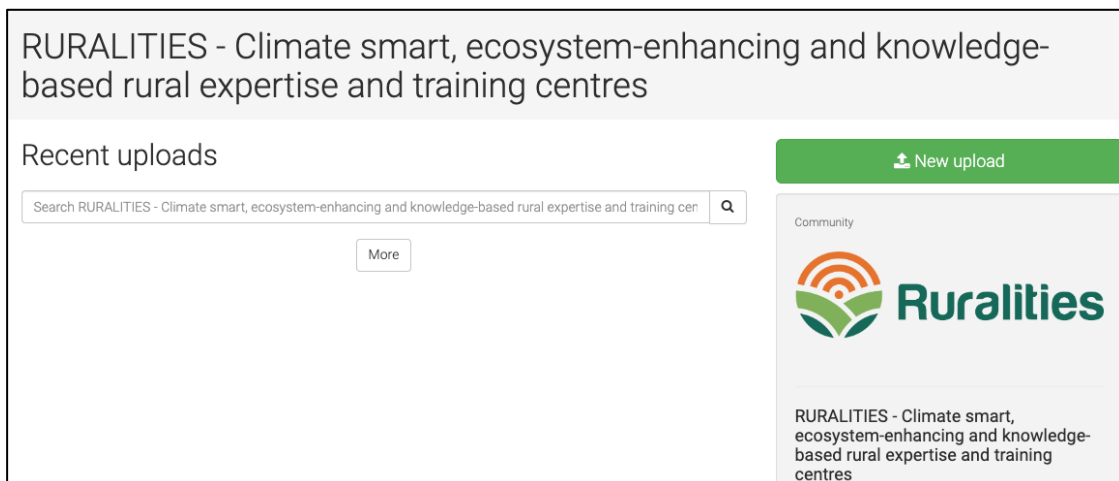
---

[4] https://guidelines.openaire.eu/en/latest/
[5] https://zenodo.org/communities/ruralities/

Figure 2. RURALITIES Community in Zenodo

7.2.4 Managing scientific publications

There are two possibilities when we want to address access to a scientific publication: publishing in green or in gold open access journals (see Section 7.4 for further clarification).

In case of green open access, Zenodo will be the repository chosen so that authors can perform the self-archiving function. For authors who already have self-archiving functions at their own institutions, they may use them instead of Zenodo, but it will be recommended that they use the Community page under Zenodo for publishing metadata pointing to the repository containing the documentation. This also allows other repositories to be used for additional dissemination of work, such as social networks or ResearchGate, which offer more limited functionalities such as open Access repository. For finding suitable green open access publishers, researchers are encouraged to consult Sherpa Romeo[6], an online resource that aggregates and analyzes publisher open access policies from around the world and provides summaries of publisher copyright and open access archiving policies on a journal-by-journal basis.

In case of gold open access, the scientific publisher's modalities for open access (e.g. embargo periods) must allow the researcher to fulfill the EC's open access obligations. Furthermore, authors should choose a publisher whose repository is, if possible, OpenAIRE-compliant, and can record a DOI for each indexed item (see sections and issue a DOI (see 7.1 and 7.2.1). For finding suitable gold open access publishers, researchers are encouraged to consult the Directory of Open Access Journals[7] (https://doaj.org/), an extensive index of diverse open access journals that use an appropriate quality control system.

7.3 Making data interoperable

Data can be made available in many different formats implementing different information models. The great variety of possibilities for implementing these information models yields enormous heterogeneity that makes interoperability of data and models difficult. The combination of standard interfaces, as well as communication protocols and data exchange models, allow us seamless integration between different platforms, projects and experimentation sites.

---

[6] https://v2.sherpa.ac.uk/romeo/
[7] https://doaj.org/

Later versions of this document will identify more types of data and the vocabularies, standards, formats or methodologies to be reused. For now, we have identified two types of data, very relevant according to the information in Table 1: Geographic information, and Agri-Food domain.

Geographical information

Considering the geographical information exchanged, the metadata vocabularies standards will be used (Dublin Core, ISO 19115 and ISO 19139) and compliance with the following regulations will be verified:

- Regulation (EU) No. 1089/2010 of the Commission of November 23, 2010 applying Directive 2007/2/EC of the European Parliament and of the Council with regard to the interoperability of the sets and spatial data services
- Regulation (EU) N° 1205/2008 of the Commission of December 3, 2008 by which Directive 2007/2/CE of the European Parliament and of the Council is executed with regard to metadata
- Regulation (EU) N° 976/2009 of the Commission of October 19, 2009 by which Directive 2007/2/CE of the European Parliament and of the Council with regard to metadata is executed

Agri-food domain

In relation to the agri-food domain, the participants in Ruralities will be inspired by the good practices offered by the DEMETER project, in which some Ruralities Partners participate. In particular, the Demeter Agricultural Information Model stands out, which spans interoperability of information among the following data domains:

- Farm data (e.g., field data, field status, soil data, Crops/treatment/fertilization data, farm input data, energy consumption data, …)
- Earth Observation Data (e.g., satellite data, remote sensing imagery, soil maps, vegetation indices, such as NDVI, EVI, NDRE, NDMI)
- Meteorological data (e.g., temperature, humidity, wind speed/direction, solar radiation, pressure, etc.)
- Agricultural machinery data (e.g., engine data, fuel consumption, emissions, exhaust gas, NO_x-conversion, exhaust temperatures)
- Representation of data quality metrics
- Field Operations data (irrigation, fertilization, soil tillage)
- Traceability data (transport)
- Livestock data
- Financial farm data, benchmarking data and KPIs
- Farmer information

DEMETER, therefore, connects dominant data systems such as FIWARE AgriFood, SAREF4AGRI, ADAPT, INSPIRE and FOODIE (Farm Oriented Open Data In Europe), AGROVOC and Earth Observation data and make them available to stakeholders.

Although in Ruralities no progress will be made in the provision of semantic information and in the field of linked data, the inclusion of qualified references to other data (from Ruralities and from previous research) will be sought.

7.4   Increase data re-use (through clarifying licenses)

According to the Grant Agreement (1.2.10 FAIR data management), experimental data is collected in laboratory record books that will be stored (or digitalized) once finished. They constitute a proof of ownership in case of

conflict and a permanent record of the work done, including experimental details and operating procedures. Entries are sufficiently detailed so that someone else could replicate the procedure. Lab books include raw data or reference to the digital location. Lab records are the basis of scientific publications, which are also published in an open access basis, making accessible the methodologies used that will enable data verification and reuse.

With regards to the scientific support of collection of experiment data, experiments can directly insert records in a database. This database can also store digitalized record books.

Databases containing experiment information will be structured to store the following data:

1. Types of data/outputs. The project activities collect, deliver, use, and reuse a vast series of public and private forms of data (surveys, events, materials reviews, etc.).
2. Findability of data/output, based on proper data protection protocols. These protocols are available via the Lean Drive Commons (SaaS platform), project website and connected platforms (community of practice, forum, etc.), and linked to the European Open Science Cloud[8], supported by well-known and open formats and software, open globally-scoped repositories such as Zenodo, DataHub[9], and EUDat[10].
3. Accessibility of data/outputs, all scientific datasets should be openly accessible (licensed using standard reuse licenses) except very specific materials related to intellectual property or privacy (GDPR), ethical matters in some cases;
4. Interoperability of data/ outputs, the project practices relevant standards for metadata and community agreed schemas, controlled vocabularies, keywords, thesauri or ontologies where possible;
5. Reusability of data/ outputs, see (2); Documentation needed to validate data analyses and facilitate data reuse will be provided in the form of readme files, codebooks, coding comments and filed definitions. Depending on the licensing, data produced in the project shall be useable by third parties, even after the end of the project.
6. Curation and storage/preservation costs

According to the EC recommendation, authors of the publication are encouraged to retain their copyright and grant adequate licenses to publishers. We include here information about the types of publication allowed, opting whenever possible for Gold Open Access:

Green open access (self-archiving)

Green open access or self-archiving means that the published article or the final peer-reviewed manuscript is archived by the researcher itself in an online repository, in most cases after its publication in the journal. The journal must grant the researcher the permission to self-archive the final peer-reviewed article, at the latest, 12 months after publication.

Gold open access (open access publishing)

Gold open access means that the publication is available by the scientific publisher as open access. Some journals require an author-processing fee for publishing open access. Author-publishing fees for gold open

---

[8] https://eosc-portal.eu/
[9] https://datahub.io/
[10] https://eudat.eu/open-access

access journals can be reimbursed within the project period and budget. Some publishers allow the researcher to deposit a copy of the article in a repository, sometimes with an embargo period.

8 ALLOCATION OF RESOURCES

Making data available according to the FAIR principle incurs costs. However, at this early stage it is not possible to provide a reasonable estimate on any additional costs, which -might result from:

- Fees associated with the publication of scientific articles in Gold Open Standards journals
- Web Site and Service Operations
- Data Archiving
- Copyright Licensing
- Data storage solutions in Ruralities repositories
- This section will be updated once reliable figures are available for the benefit of future activities.

We already consider that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

The management of data in Ruralities is carried out through the provisioning of relevant tools and systems (such as GDrive, CKAN or Zenodo) that provide the required level of fairness towards data sharing, security and privacy. Data management and data governance functions in this project is a collaborative task, in which all partners participate. Therefore, each partner is responsible for their own data, and they constitute the data owners. The coordinator will take the lead role in establishing the procedures and monitoring the utilization of available infrastructure.

We want to differentiate at this point the concepts of *owners/responsible for the data*, from *owner/responsible for the available infrastructure to manage the data*. For example, the SaaS platform that we use at Ruralities for file storage and communication between partners, is based on Google Drive, and managed directly by P1, who owns the repository, but delegates its editing to all partners for a smoother operation. The owners of the different data management tools, such as the data repository (CKAN), Zenodo community, and communities of practices will be defined throughout the execution of the project and indicated in future updates of this DMP.

9 DATA SECURITY

Related to data security in the Project repositories, we highlight the access permission system defined for Ruralities:

- Ruralities SaaS Platform (called Lean Drive Commons, LeanDC, in the GA): All documents have two types of access, configurable in each case. Open access allows any holder of the permanent link to access the data. Access by invitation requires an email from the guest, and access is only allowed with the credentials of the invited user (using in this case the Google credentials system). When a file is shared with an individual or group, the owner can choose what they can do with it: (A) Viewer: They can view but can't change or share the file with others, (B) Commenter: They can make comments and suggestions but can't change or share the file with others, (C) Editor: They can make changes, accept or reject suggestions, and share the file with others. Best practices for sharing in Ruralities SaaS are extracted from well stablished documentation[11].
- Ruralities Data Repository: The authorization system used by this component is based on CKAN's authorization system[12], which controls which users are allowed to carry out which actions on the site. For example, the authorization system controls who can register new user accounts, delete user accounts, or create, edit and delete datasets, groups and organizations. In addition to traditional organization-based permissions, the Data Repository can also enable the dataset collaborators feature, which allows dataset-level authorization. This provides more granular control over who can access and modify datasets that belong to an organization, or allows authorization setups not based on organizations. It works by allowing users with appropriate permissions to give permissions to other users over individual datasets, regardless of what organization they belong to.
- Official Website: The content management system of the Ruralities platform is based on a WordPress environment. The WordPress system is a content management system (CMS) that defines access credentials according to user roles. We have the administrator user, who can manage the entire system, activate server updates, install extensions, and create user accounts. Another user is the Publisher User, who has permissions in the CMS to create content on the web page. Create news, modify menus, and include files and multimedia information. Finally, we have the Guest user, who can access the ecosystem, but without write permissions (he can read everything published but the only way to make changes to the content of the page is to propose them to an editor or administrator type user).

Related to data storage and protection. The following guidelines will be followed in order to ensure the security of the data:

- Store data in at least two separate locations to avoid loss of data;
- Encrypt data if it is deemed necessary by the participating researchers;
- Limit the use of USB flash drives.
- Label files in a systematically structured way in order to ensure the coherence of the final dataset.

All project deliverables and data will be stored and shared in the SaaS platform (Google Drive repository) restricted to the project consortium. As an initial step, only the Consortium Partners will have access to the cloud storage where dataset and metadata are filed. Following, scientific publications and articles, the dataset

---

[11] University of Michigan: Best Practices for Sharing in Google Drive. Available at: https://documentation.its.umich.edu/google-drive-sharing
[12] CKAN's Authorization: https://docs.ckan.org/en/2.9/maintaining/authorization.html

deliverables and the final demonstrator research results will be shared through Zenodo and other database to promote the data making FAIR.

For the case studies involving the collection of private information through mobile applications or surveys, such as the location of the users during the experiments, the test users will be asked for written authorization for the collection of the anonymized data and the use will be explained to them. To provide this authorization the "Informed Consent Form" of Annex 2 will be used. To avoid suspicions of inappropriate use of anonymized information, such as techniques for determining the "digital footprint" (traceable digital activities, actions, contributions and communications), the technique of periodic change of identifiers will be used for large collections, through which users will gradually adopting different digital identities that make the use of this type of technique impractical.

Finally, related to data retention and destruction, GDPR data retention rules[13] require any personal data that is collected or processed to be kept only for as long as data are required to achieve the purpose for which the information was collected, although there are exceptions – scientific or historical research for example. Partners and third parties have the right to submit a data subject request, under the provisions of the GDPR, with the purpose to access or correct their own information. Annex 4 contains the template for the Data subject request form.

From a technical point of view, and for the management of authorized private information, servers associated with the data management points of contact will be used to store data that, for greater security, will be encrypted using the 256-bit AES algorithm. At the end of the program and once the data is no longer required to achieve the purpose which the information was collected, a state-of-the-art data erasing method will be used to securely erase the contents of the hard drives. Since open-source tools are available, there will be no extra costs associated with applying cryptographic algorithms and subsequent destruction of data.

---

[13] https://www.netsec.news/gdpr-data-retention/

10 ETHICAL AND LEGAL FRAMEWORK

The project has a WP dedicated to Ethics: "measures to ensure an ethical framework", which defines the following outcomes:

- D3.1 – Ruralities Ethics Appraisal Scheme
- D3.2 – Report on the framework for human participation animal ethics, environment, health and safety, initial version
- D3.3 – Report on the framework for human participation animal ethics, environment, health and safety, updated version

WP-3 has the objective of generating a comprehensive framework to secure the project development and results abides the ethical framework of the Horizon Europe Programme (HEP) guiding principles, gathered in the 'Ruralities Ethics Appraisal Scheme'. WP-3 consider all key HEP Ethic features:

1) Human (H, requirement 1);
2) Protection of Personal Data (POPD, requirement 2);
3) Animal welfare (framework for animal ethics);
4) Third Countries (well represented in the consortium);
5) Environment, health, and safety.

Ethical issues will be addressed by Ruralities Project Management Office, in conjunction with the project Advisory Board. Focus will be put on the compliance with existing ethical and legal framework for safeguarding human (European Union Directive 2010/63/EU) and animal welfare and care of experimental animals (European Union Directive 2010/63/EU)[14].

Proposed solutions in Ruralities do not expose, use or analyze personal sensitive data for any purpose. In this respect, no ethical issues related to personal sensitive data are raised by the technologies to be employed in the planned pilots. Furthermore, the Ruralities consortium considers during the project lifetime the ethical rules and standards of Horizon programme, and those reflected in the Charter of Fundamental Rights of the European Union. Generally speaking, ethical, social and data protection considerations are crucial and are given all due attention.

Besides these general conditions, the consortium is aware that a number of privacy and data protection issues could be raised by the activities (i.e. in all Demonstrator activities) to be performed in the scope of the project. Therefore, each individual partner will report to their individual ethical authority (Work package leader or assigned individual) on a quarterly basis to identify ethical issues that may arise or have arisen. The PMO will then action this item for review and report back to work package leader as to the necessary recommendations.

The task that defined ethics quality assurance and control measures (e.g., a set of training to the partners, guidelines and data collection and monitoring methods on the specific related issues identified in Ruralities) is the T3.1 – 'Ruralities Ethics Appraisal Scheme'. This task also defines and communicates the ethical dimension integration into WP measures to assess potential additional issues during the progress of the project.

---

[14] European Union Directive 2010/63/EU https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010L0063

10.1 Additional Local Legislation of countries involved within Ruralities

In this subsection we provide a study of the main national legislations of the countries participating in Ruralities, both in Europe and in the African continent.

In general, for all national legislations, personal data is defined as any information that relates to an identified or identifiable natural person. National laws provide data subjects with a number of rights, including the right to access their personal data, the right to rectify or erase their personal data, and the right to object to the processing of their personal data.

Also, national laws also impose certain obligations on data controllers and processors, including the obligation to obtain the data subject's consent for the processing of their personal data, the obligation to implement appropriate technical and organizational measures to protect personal data, and the obligation to notify the competent authority and data subjects in case of a personal data breach.

The national laws of the participating countries are listed below, arranged alphabetically:

Belgium

The Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data ('the Act)[15] applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in Belgium.

Belgian DPA was established by the Act of 3 December 2017 Establishing the Data Protection Authority (as amended) (only available in Dutch here) ('the DPA Law') and replaced its predecessor, the Privacy Commission, on 25 May 2018. The Act grants the data subject and the Data Protection Authority ('Belgian DPA') the right to obtain a cease-and-desist order against a company infringing the data protection laws.

Burkina Faso

The most relevant law in Burkina Faso in relation to data protection is the Act No. 001-2021/AN of 30 March 2021 (available in French)[16].

The 2021 Act strengthens the protection of the privacy of individuals, including by broadening its geographical scope to offshore data controllers who carry out processing operations from Burkina Faso (irrespective of whether they use local means of processing), by supervising transborder transfers, and by providing a more comprehensive right to be informed. In addition, the 2021 Act reinforces security requirements with the obligation, where data is transferred to a third country, to enter into a contract with the data recipient that includes a return of data clause and to encrypt the data, and introduces the principle of data localization, with the obligation to host health data in the Country.

Côte d'Ivoire

Cote D'Ivoire law regarding personal data protection is N°2013-450 from 19 June 2013, "Relative a la Protection des Données a Caractère Personnel"[17]

This reference text provides important principles in the processing of personal data. There are provisions in this law with which companies and data controllers must comply, examining their systems and their processes

---

[15] https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf
[16] https://www.dataguidance.com/jurisdiction/burkina-faso
[17] http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/104182/126984/F366961585/CIV-104182.pdf

for processing the personal data of their customers or prospects in order to ensure their compliance with the law.

The Ivorian law relating to the protection of personal data provides in its article 39 that "the processing of personal data is confidential. It is carried out exclusively by persons who act under the authority of the controller and only on his instructions. The data controller (the employer) is required to take every precaution with regard to the data, in particular to ensure their security, and to prevent them from being deformed, damaged, or from third parties having access to them.

The data controller must determine and implement the "technical and organizational" measures necessary to ensure the confidentiality of employees' personal data in order to avoid any disclosure.

Croatia

From 25 May 2018, the overall concept of personal data protection in the Republic of Croatia is regulated by the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the General Data Protection Regulation Implementation Act 2018 (available only in Croatian[18]) ('the Act'), which in effect represents a new and stronger mechanism for personal data protection. While most provisions and rules for data protection are found in the GDPR and the Act, there are other national statutes and bylaws which prescribe specific rules for data processing and use.

The Personal Data Protection Agency ('AZOP') issues and publishes data protection guidance[19]. In addition, the AZOP has published numerous additional opinions, recommendations, and clarifications on specific data processing issues and provided useful links to guidelines issued by the European Data Protection Board ('EDPB') (all available on the AZOP's official website in Croatian)[20].

Cyprus

In Cyprus the law supplementing the GDPR is the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018). This law was published in the official gazette of the Cyprus Republic, On 31 July 2018.

The law was adopted for the effective implementation of certain provisions of the Regulation (EE) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), which applies as of 25 May 2018. An unofficial English translation of the Law can be found[21].

Upon entry into force of the provisions of the law 125(I)/2018, the Processing of Personal Data (Protection of Individuals) Law of 2001 (Law 138(I)/2001) was repealed.

Democratic Republic of the Congo

---

[18] https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html
[19] https://azop.hr/national-legislation/
[20] https://azop.hr/
[21] https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/2B53605103DCE4A4C225826300362211

The Democratic Republic of the Congo (DRC) currently does not have a specific data protection law that is solely focused on the protection of personal data. However, several laws and regulations in the country provide some level of protection for the privacy and personal data of its citizens.

The DRC Constitution[22] guarantees the right to privacy, and the protection of personal data is also addressed in various laws, such as the Law on Telecommunications, the Law on Electronic Transactions, and the Law on Personal Data.

The Law on Telecommunications (Law No.20/017)[23] regulates the processing of personal data in the context of telecommunications, while the Law on Electronic Transactions addresses the protection of personal data in the context of electronic transactions. The Law on Personal Data, which was enacted in 1999, provides for the protection of personal data, including the right to access and rectify personal information.

Furthermore, the DRC has ratified the African Union Convention on Cyber Security and Personal Data Protection, which is a regional legal framework for the protection of personal data in Africa.

Overall, while the DRC does not have a specific data protection law, its Constitution and other laws provide some level of protection for the privacy and personal data of its citizens. However, there is a need for more comprehensive legislation to address the growing importance of data protection in today's digital world.

Denmark

The most relevant law in Denmark in relation to data protection is the EU General Data Protection Regulation (GDPR), came into effect on May 25, 2018, stablishing a single, comprehensive framework for the protection of personal data within the European Union, including Denmark.

In addition to the GDPR, Denmark has its own national data protection law, the Danish Data Protection Act (Lov om behandling af personoplysninger)[24], which supplements and implements the GDPR's requirements at a national level. The Danish Data Protection Act also regulates the processing of personal data by public authorities in Denmark.

In addition to the GDPR and the Danish Data Protection Act, Denmark has also implemented the ePrivacy Directive into national law through the Act on Processing of Personal Data in Electronic Communications (Lov om behandling af personoplysninger i elektroniske kommunikationsnet og -tjenester)[25], which regulates the use of cookies and similar technologies, as well as unsolicited electronic marketing.

Egypt

Egypt recently introduced the Law on the Protection of Personal Data (the "Data Protection Law") issued under Resolution No. 151 of 2020 (only available in Arabic[26]) (the "Resolution") on July 13, 2020.

The Data Protection Law reflects the European General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), as it aims to establish various standards and rules that safeguard the rights of individuals in Egypt regarding their personal data. Prior to the introduction of the Data Protection Law, data protection was only governed through various legislations in Egypt, such as the Constitution of the Arab Republic of Egypt (the

---

[22] https://wipolex.wipo.int/en/text/492212

[23] https://legalrdc.com/2020/11/25/loi-n-20-017-du-25-novembre-2020-relative-aux-telecommunications-et-aux-technologies-de-linformation-et-de-la-communication/

[24] https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf

[25] https://w2l.dk/file/377959/engelsk-vejledning-cookiebekendtgorelse.pdf

[26] https://www.dataguidance.com/sites/default/files/egypt_data_protection_law.pdf

"Constitution'), the Penal Code No. 58 of 1937 (the "Penal Code;) and the Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes (only available in Arabic[27]) (the "Cybersecurity Law"). With the passing of the Data Protection Law, all of Egypt's rules and regulations about data protection and privacy are now in one place.

In addition to the Personal Data Protection Law, Egypt has also implemented the ePrivacy Directive into national law through the Electronic Signature Law, which regulates the use of electronic signatures, and the Law on Regulating the Use of Information Networks and Information Technology, which sets out rules for the protection of personal data in electronic communications.

Ghana

The most relevant law in Ghana in relation to data protection is the Data Protection Act[28], which was enacted in 2012. The law provides a legal framework for the protection of personal data in Ghana and applies to all data controllers and processors who process personal data in Ghana, regardless of whether they are based in Ghana or not.

In addition to the Data Protection Act, Ghana has also implemented the ePrivacy Directive into national law through the Electronic Communications Act, which regulates the use of electronic communication and the protection of personal data during electronic communication.

Hungary

The national regulation in Hungary is the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information. This act is also available in English[29].

The object of this Act is to define the fundamental rules for controlling data to ensure that the data controllers respect the private sphere of natural persons and to achieve transparency in public affairs through the enforcement of rights to access and disseminate data of public interest and data public on grounds of public interest.

The act defines personal data as "data relating to the data subject, in particular, their name and identification number, as well as one or more factors specific to their physical, physiological, mental, economic, cultural or social identity as well as conclusions drawn from the data concerning the data subject."

The scope of this Act covers all data control and data processing activities performed in Hungary relating to the data of natural persons, as well as data of public interest and data public on grounds of public interest.

Italy

Italy adopted the Italian Personal Data Protection Code (the Code)[30] with an amendment to comply to General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). The Code manages data subjects' complaints, provides specific data protection measures for data controllers and processors and adopts guidelines to assist organizations' compliance with personal data protection laws.

---

[27] https://www.dataguidance.com/sites/default/files/175-2018.pdf
[28] https://www.dataguidance.com/sites/default/files/data_protection_act_2012_act_843.pdf
[29] https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2012)021-e
[30] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9740796

Decree was published in the Italian Official Gazette on 4 September 2018 (coming into effect on 19 September 2018)[31] and repealed those sections of the Code – stemming from the implementation of the previous Data Protection Directive (Directive 95/46/EC) – which were directly conflicting with the GDPR. Furthermore, the Decree introduced a number of new provisions as a consequence of the GDPR.

Kenya

To give effect to Article 31(c) and (d) of the Constitution, the Kenyan parliament stablishes the Data Protection Act[32] in 2019. This Act stablishes the Office of the Data Protection Commissioner; to make provision for the regulation of the processing of personal data; to provide for the rights of data subjects and obligations of data controllers and processors; and for connected purposes.

The purpose of this Act is (a) to regulate the processing of personal data; (b) to ensure that the processing of personal data of a data subject is guided by the principles set out in Section 25; (c) to protect the privacy of individuals; (d) to establish the legal and institutional mechanism to protect personal data; and (e) to provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with this Act.

Malawi

The most relevant law in Malawi in relation to data protection is the Electronic Transactions and Cybersecurity Act (ETCA), which was enacted in 2016. The ETCA provides a legal framework for the protection of personal data in Malawi and applies to all data controllers and processors who process personal data in Malawi, regardless of whether they are based in Malawi or not.

In addition to the ETCA, Malawi has also implemented the ePrivacy Directive into national law through the Communications Act, which regulates the use of electronic communication and the protection of personal data during electronic communication.

Mauritania

The main law in Mauritania in data protection is the Law 2017-020, 22 July 2017 of the protection of personal data (sur la protection des données à caractère personnel[33]). The purpose of this law is to put in place a normative and institutional framework for the processing of personal data, with a view to guaranteeing better services and protecting against breaches of privacy, likely to be caused using Information and Communication Technologies.

Apart from this law, the Council of Ministers met on Wednesday, December 15, 2021, adopted the following two draft decrees[34]:

- Draft decree relating to the retention of electronic data and filtering. Defines certain procedures related to the retention of data, the conditions of judicial requisitions and administrative requests for access to data from service providers, as well as the filtering and identification obligations of the authorities concerned by the granting of access licenses and authorizations and the blocking or deletion of illegal content, according to a specific mechanism.

---

[31] https://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg
[32] https://www.odpc.go.ke/download/kenya-gazette-data-protection-act-2019/
[33] https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/112890/141188/F-1939462947/MRT-112890.pdf
[34] https://ami.mr/fr/Depeche-61831.html/

- Draft decree relating to the composition, organization and functioning of the personal data protection authority. Establish a personal data protection authority responsible for ensuring that the processing of personal data takes place in Mauritania while determining the composition of this authority and the procedures for appointing its members.

Morocco

In Morocco, personal data protection is governed by Law n° 09-08 of 18 February 2009 (in French[35]), relating to the protection of individuals with respect to the processing of personal data and by its Implementation Decree n° 2-09-165 of 21 May 2009 (in French[36]).

The law was initially enacted to encourage foreign investment, including the offshoring and outsourcing of processing activities related to European residents' personal data. Morocco is, indeed, an important player in the offshoring and outsourcing market due to its proximity to European markets as well as its competitive telecommunication infrastructure and multilingual workforce.

Mozambique

Mozambique does not have a specific law that is solely focused on data protection. However, the country's Constitution[37], as well as several other laws and regulations, provide some protection for the privacy and personal data of its citizens.

The Mozambican Constitution guarantees the right to privacy, and the protection of personal data is also addressed in various laws, such as the Civil Code, the Electronic Transactions Law[38], and the Cybersecurity Law.

The Civil Code includes provisions on the protection of personal data, including the right to privacy and the right to access and rectify personal information. The Electronic Transactions Law regulates the processing of personal data in the context of electronic transactions, while the Cybersecurity Law sets out measures for the protection of information and communication systems.

Furthermore, Mozambique has ratified the African Union Convention on Cyber Security and Personal Data Protection, which is a regional legal framework for the protection of personal data in Africa.

Nigeria

Nigerian Data Protection Regulation[39], 2019 (NDPR) issued by the National Information Technology Development Agency ('NITDA').

The NDPR makes provision for the rights of data subjects, the obligations of data controllers and data processors, transfer of data to a foreign territory amongst others. In particular, the objective of the regulation is as follows:

---

[35] http://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf

[36] http://www.cndp.ma/images/lois/Decret-2-09-165-Fr.pdf

[37] https://constitutions.unwomen.org/en/countries/africa/mozambique

[38] https://www.dataguidance.com/sites/default/files/electronic_transactions_law.pdf

[39] https://www.dataguidance.com/sites/default/files/nigeriadataprotectionregulation11.pdf

a) to safeguard the rights of natural persons to data privacy; b) to foster safe conduct for transactions involving the exchange of Personal Data; c) to prevent manipulation of Personal Data; and d) to ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice.

Romania

In Romania the authority for data protection is the National Supervisory Authority for the Processing of Personal Data[40]. It works as an autonomous central public authority with general competence in the field of personal data protection, representing the guarantor of respect for the fundamental rights to private life and the protection of personal data, established especially by art. 7 and 8 of the Charter of Fundamental Rights of the European Union, art. 16 of the Treaty on the Functioning of the European Union and of art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

The laws that are the fundament for general data protection in Romania are, besides the EU 2016/679 Regulation:

- LAW no. 190 of July 18, 2018 regarding implementation measures of EU 2016/679 Regulation of the European Parliament and of the Council of April 27, 2016 regarding the protection of natural persons as in processing of personal data and regarding free movement of these dates and the repealing of Directive 95/46/EC (General Regulation on data protection).

- LAW No. 129 of 15 June 2018 on amending and supplementing the Law No 102/2005 on the establishment, organisation and functioning of The National Supervisory Authority for the Processing of Personal Data, and for the repeal of Law no. 677/2001 for the protection persons with regard to the processing of personal data and free movement of such data.

Rwanda

The Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy ('the Data Protection Law')[41] was published in the Official Gazette on 15 October 2021. The law provides a legal framework for the protection of personal data in Rwanda and applies to all data controllers and processors who process personal data in Rwanda, regardless of whether they are based in Rwanda or not.

In addition to the Law on the Protection of Personal Data, Rwanda has also implemented the ePrivacy Directive into national law through the Law N° 36/2018 of 09/08/2018 relating to the Protection of Persons using Electronic Communications and Transactions. This law regulates the use of electronic communication and the protection of personal data during electronic communication.

Senegal

The principal data protection legislation is Law no. 2008-12 dated 25 January 2008 relating to the protection of personal data (Data Protection Act) ("DPA")[42], decree no. 2008-721 dated 30 June 2008 relating to the application of the DPA, and Law no. 2016-29 dated 8 November 2016 modifying the penal code. The DPA and its application decree provide the conditions relating to data processing, the rights of Data Subjects and the obligations of Data Controllers.

---

[40] https://www.dataprotection.ro/
[41] https://www.dataguidance.com/sites/default/files/rw-government-gazette-dated-2021-10-15-no-special.pdf
[42] https://www.wipo.int/wipolex/en/legislation/details/6229

Funded by the European Union

The DPA creates the Senegalese Data Protection Authority (Commission de Protection des Données Personnelles) ("CDP") Law no. 2016-29 dated 8 November 2016 modifying the penal code, which provides criminal offences relating to data processing and the applicable sanctions.

Serbia

The most relevant law in Serbia in relation to data protection is the Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti)[43] which was adopted on 21 November 2018 and became effective on 21 August 2019. The Law on Personal Data Protection is in line with the EU General Data Protection Regulation (GDPR).

In addition to the Law on Personal Data Protection, Serbia also has a Law on Electronic Document, Electronic Identification and Trusted Services in Electronic Commerce, which regulates the use of electronic signatures, and a Law on Electronic Communications, which regulates the processing of personal data in the context of electronic communications.

Slovakia

The main data protection regulation in Slovakia is the Act of 29 November 2017 on personal data protection[44].

This Act regulates: (a) Protection of the rights of natural personas against unauthorized processing of their personal data; (b) right, obligations, and responsibility during processing of personal data of natural persons; (c) status, activity and organization of the Office for Personal Data Protection of the Slovak Republic.

In addition to the GDPR, the Act also implements the Data Protection Directive with respect to Law Enforcement (Directive (EU) 2016/680).

Slovenia

The Slovenian Personal Data Protection Act (ZVOP-2)[45] regulates the right to the protection of personal data, obligations, principles, entitlements, procedures and measures that ensure constitutional compliance, legality and justification of interference with privacy, dignity, secrecy of personal data, data self-determination or other fundamental rights of the individual.

ZVOP-2 manages the processing of personal data and the rules on the free flow of personal data for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals in the processing of personal data and on the free flow of such data and on the repeal of Directive 95/46/EC (General Data Protection Regulation), and other issues of personal data processing and protection.

Spain

The Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (LOPD-GDD)[46] is an organic law approved by the Cortes Generales of Spain whose objective is to adapt Spanish internal law to the Regulation General of Data Protection. This organic law repeals the previous Organic Law

---

[43] https://www.poverenik.rs/images/stories/dokumentacija-nova/zakoni/ZZPLnovembar2018/ZZPLnovembar2018.doc
[44] https://dataprotection.gov.sk/uoou/en/content/national-legislation
[45] http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO7959#
[46] https://www.hacienda.gob.es/es-ES/El%20Ministerio/Paginas/DPD/Normativa_PD.aspx

Funded by the European Union

15/1999 on the Protection of Personal Data, which was based on article 18 of the Spanish Constitution on the right to family and personal privacy and the secrecy of communications.

Organic Law 3/2018 has been prepared in accordance with the General Data Protection Regulation (RGPD). In addition to these laws. Subsequently, laws have appeared that complement the law in force, such as Organic Law 7/2021, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions, and Law 2/2023, regulating the protection of people who report on regulatory violations and the fight against corruption.

Sudan

Sudan currently does not have a specific data protection law that is solely focused on the protection of personal data. However, the country has some legal provisions that address data protection in various laws and regulations.

The Sudanese Constitution[47] recognizes the right to privacy and the protection of personal information, and this right is also affirmed in other laws such as the Penal Code and the Electronic Transactions Act.

The Electronic Transactions Act, enacted in 2014, provides some protection for personal data in electronic transactions, including provisions on the protection of personal information, the confidentiality of electronic messages, and the use of electronic signatures.

The Penal Code also includes provisions related to the protection of privacy and personal information, including criminalizing the unauthorized access, interception, and disclosure of personal data.

In addition, Sudan has ratified the African Union Convention on Cyber Security and Personal Data Protection, which is a regional legal framework for the protection of personal data in Africa.

Tanzania

The most relevant law in Tanzania in relation to data protection is the Data Protection Act, 2019. The act was enacted on 1st May 2020 and was assented by the President of Tanzania into DPA law[48]. provides for matters relating to protection of personal data and establishes the principles guiding and conditions for collection and processing of personal data.

In addition to the Data Protection Act, Tanzania has also implemented the ePrivacy Directive into national law through the Electronic and Postal Communications Act, 2010 which regulates the use of electronic communication and the protection of personal data during electronic communication.

Togo

The most relevant law in Togo in relation to data protection is the Personal Data Protection Act[49], which was enacted in 2019. The law provides a legal framework for the protection of personal data in Togo and applies to all data controllers and processors who process personal data in Togo, regardless of whether they are based in Togo or not.

---

[47] https://www.constituteproject.org/constitution/Sudan_2019.pdf?lang=en
[48] https://www.dlapiperdataprotection.com/index.html?t=law&c=TZ#:~:text=On%2027%20November%202022%2C%20the,and%20processing%20of%20personal%20data
[49] https://jo.gouv.tg/sites/default/files/JO/JOS_29_10_2019-64E%20ANNEE-N%C2%B026%20TER.pdf#page=1

In addition to the Personal Data Protection Act, Togo has also implemented the ePrivacy Directive into national law through the Electronic Communications Act, which regulates the use of electronic communication and the protection of personal data during electronic communication.

Tunisia

The most relevant law in Tunisia in relation to data protection is the Organic Law on the Protection of Personal Data (OLPPD)[50], which was enacted in 2019. The law provides a legal framework for the protection of personal data in Tunisia and applies to all data controllers and processors who process personal data in Tunisia, regardless of whether they are based in Tunisia or not.

In addition to the OLPPD, Tunisia has also implemented the ePrivacy Directive into national law through the Telecommunications Act, which regulates the use of electronic communication and the protection of personal data during electronic communication.

Turkey

The most relevant law in Turkey in relation to data protection is the Personal Data Protection Law (Kişisel Verilerin Korunması Kanunu)[51], which was adopted on 24 March 2016 and became effective on 7 April 2016. The Personal Data Protection Law is based on the EU General Data Protection Regulation (GDPR) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

In addition to the Personal Data Protection Law, Turkey has also implemented the ePrivacy Directive into national law through the Law on the Regulation of Electronic Commerce (Elektronik Ticaretin Düzenlenmesi Hakkında Kanun)[52], which regulates the use of cookies and similar technologies, as well as unsolicited electronic marketing.

Uganda

The most relevant law in Uganda for data protection is the Data Protection and Privacy Bill[53], from 2015. The object of this Bill is to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the right of the persons whose data is collected and the obligations of data collectors, data processors and data controllers, to regulate the use or disclosure of personal information; and for related matters.

The Bill seeks to give effect to article 27(2) of the Constitution by providing for the principles of data protection and recognizing the rights of the persons from whom personal information is collected.

United Kingdom

The Data Protection Act 2018[54] is the UK's implementation of the General Data Protection Regulation (GDPR), which have been granted EU adequacy. The provisions of the EU GDPR have been incorporated directly into UK law as the UK GDPR. In practice, there is little change to the core data protection principles, rights and obligations. GDPR recitals add depth and help to explain the binding articles. Recitals continue to have the

---

[50] http://www.inpdp.nat.tn/ressources/loi_2004.pdf

[51] https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law

[52] https://www.cailliau-colakel.av.tr/tr/new-legislation-on-the-regulation-of-electronic-commerce-3/

[53] https://www.parliament.go.ug/cmis/views/929c2b83-72d9-41a4-a901-8edfab1ea464%25253B1.0

[54] https://www.gov.uk/data-protection

Funded by the European Union

same status as before – they are not legally binding; they are useful for understanding the meaning of the articles.

Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage.

Zambia

The most relevant law in Zambia in relation to data protection is the Data Protection Act[55], No. 3 of 2021. This law was assented the 23rd of March, 2021, and enacted by the Parliament of Zambia the following day. It provides a legal framework for the protection of personal data in Zambia. It provides an effective system for the use and protection of personal data; regulate the collection, use, transmission, storage and otherwise processing of personal data; establish the Office of the Data Protection Commissioner and provide for its functions; the registration of data controllers and licensing of data auditors; provide for the duties of data controllers and data processors; provide for the rights of data subjects; and provide for matters connected with, or incidental to, the foregoing.

In addition to the Data Protection Act, Zambia has also implemented the ePrivacy Directive into national law through the Electronic Communications and Transactions Act, 2009. This law regulates the use of electronic communication and the protection of personal data during electronic communication.

---

[55] https://www.dataguidance.com/sites/default/files/act_no._3_the_data_protection_act_2021_0.pdf

11 CONCLUSIONS

This document describes the main principles and guidelines for the Data Management for the Ruralities project, in line with Horizon Europe open data requirements and FAIR (Findable, Accessible, Interoperable and Reusable) principles. FAIR policy, in that sense, defines comprehensible procedures and responsibilities to embed data management activities in the complete project lifecycle.

In addition, the main contributions of this deliverable are the overview of the characteristics of data to be collected in Ruralities, considering all tasks, and the security and legal framework, which is complemented with a study of local legislations of countries involved in Ruralities, to determine if the local data protection policies have similarities to the European GDPR definitions.

As living document, the DMP will be updated throughout the project lifetime. Further updating of the Data Management Plan will include the up-to-date version of the Ruralities data repositories: SaaS Platform, Data Repository, and Official Website, among others.

ANNEX 1 DATA COLLECTION TEMPLATES

We include here the two templates to collect information from task leaders about the tasks they lead. Figure 3 shows the template for collecting the characteristics of data to be collected in Ruralities, which have allowed the results presented in Table 1 to be generated.

Expected data in Ruralities (for M6 DMP deliverable). For task leaders.

If you are a task leader, please, fill this form with your vision and the information you have about the task that you are leading.
Please <u>complete the form for each task that you lead</u>. Even if the task starts in the next few years, please fill out this form as many times as the tasks you lead.

The form is related to the data that is going to be used and/or collected at task level. Do not hesitate to ask as many questions or doubts you need.

* Required

1. Partner (name, acronym or number) *

    _____

2. Which task are you leading? *

    _____

3. Data description or collection method *

    Please, describe what kind of data are you gonna manage in the task you are leading, and how they would be collected.
    For example:

    - Minutes from meetings with experts and/or project partners. Notes taken by the task leader after every meeting
    - Reports about the rural landscape. Each partner must provide a report about its own country
    - Surveys, using Google forms, including internal and external participants
    - Other: Online survey, spreadsheet via consortium, selection of showcases, minutes and reports from workshops, SIMSES' meetings, desk research, etc. Please, elaborate as much as possible.

4. Data utility (objective) *

    Please, describe the final purpose of the data you expect to collect
    For example:

    - Identify challenges to be addressed in the rural areas
    - Define some criteria and requirements for task X
    - Create a catalogue of good practices to inspire project partners and external participants
    - Investigate and understand the evolution of innovation and policy making activites
    - Monitor skill developments
    - Score the performance of EU food systems
    - Etc. (Please elaborate as much as possible)

5. Data format *

    Please, describe the type and/or format of data
    For example: Word files, Excel files, PDF, SQL databases, Audio/Video files (MP3, MP4), etc.

Figure 3. Template for collection of data characteristics for each task

Figure 4 shows the collection template of the additional Local Legislation of countries involved within Ruralities, which have generated the results shown in Section 10.1.

Data protection in Ruralities project

Please, fill this form with the best of your knowledge. Do not hesitate to ask as many questions or doubts you need.
/ Veuillez remplir ce formulaire au mieux de vos connaissances. N'hésitez pas à poser autant de questions ou de doutes que nécessaire.

* Required

1. Partner (name, acronym or number) *
   / Partenaire (nom, acronyme ou numéro)

   _____

2. In which country are you developing your research or activities? *
   / Dans quel pays développez-vous vos recherches ou activités ?

   _____

3. Is there any national or international regulation in your country protecting citizens private data? Please *
   research this.
   / Existe-t-il une réglementation nationale ou internationale dans votre pays protégeant les données
   privées des citoyens ? Veuillez rechercher ceci.

   By data protection regulation we mean any local legislation allowing citizens to better control their personal data,
   extending/transposing GDPR, or any other related law or directive.
   / Par réglementation sur la protection des données, nous entendons toute législation locale permettant aux citoyens
   de mieux contrôler leurs données personnelles, étendant/transposant le RGPD, ou toute autre loi ou directive
   connexe.

   Mark only one oval.

   ◯ Yes
   ◯ No

4. Please, if you answered "yes" to the previous question, give us as many details as you can about this
   regulation (official name, acronym or identifier, short description, link, etc.)
   / S'il vous plaît, si vous avez répondu "oui" à la question précédente, donnez-nous autant de détails que
   possible sur ce règlement (nom officiel, acronyme ou identifiant, description courte, lien, etc.)
   For example, spanish "Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal" or
   french "Décret n° 2019-536 du 29 mai 2019"

Figure 4. Template for collection of local legislation of participating countries

ANNEX 2 INFORMED CONSENT FORM

In this Annex we include the informed consent form defined in the RURALITIES scope that will be used by partners to request rights to use personal information, and its management, during the execution of activities with external stakeholders.

Text in red color contains guidelines for adjusting this template and should be deleted.

Text included in < > and/or highlighted with grey should be replaced with content that is suitable to the context of each activity & project as well as to the organisation seeking to obtain the consent.

Before using this template take the time to carefully read and adjust it to the needs of the activity at hand as well as to any relevant regulations and particularities applicable to your country and organisation. Specifically, this template has been developed for a data processing activity involving interviews, however you can easily adapt it to other common data processing activities such as surveys, events organizing, etc.

INFORMED CONSENT FORM

Who we are:

We are < Insert Partner Name > and we are contacting you in the framework of RURALITIES, a project funded by the European Union under the Horizon Europe Research and Innovation funding programme. A detailed description on how RURALITIES handles personal data is presented in the project's Privacy policy that accompanies this Consent Form.

Project: RURALITIES - Climate smart, ecosystem-enhancing and knowledge-based rural expertise and training centres (GA Number 101060876).

Partner:

Organisation name: < Insert Partner Name >

Address: < Insert Partner Address >.

Phone: < Insert Partner Phone >.

E-mail: <Insert Partner Generic E-mail Address >

Responsible persons:

You may delete the line referring to the Data Protection Officer if your organisation does not have one.

#	Role	Name	E-mail

1	RURALITIES Project Manager	\<Insert name of project manager\>	\<Insert email of project manager\>
2	Interviewer	\<Insert name of interviewer\>	\<Insert e-mail of interviewer\>
3	Data Protection Officer	\<Insert name of DPO \>	\<Insert e-mail of DPO \>

What do we need from you?

Please explain in a brief paragraph (4-5 lines) the activity and its purpose under the frame of the project.

Example: We need you to participate in an interview that will be carried out by RURALITIES with a view to validate ….

The interview is expected to last for no more than < Insert number of minutes > minutes. We will take written notes and we will be making a sound recording of the interview.

Please adapt the following text to accurately depict the type of personal data to be collected.

To effectively conduct this interview, we need to process some of your personal data:

- Your contact details (full name, email, phone number);

- Some basic demographics (age, gender);

- Your professional info (organization, job position, field of expertise);

- Your opinions on the subject matter.

Why do we need your data & what will we do with them?

We need your data to contact you in order to plan and carry out the aforementioned interview and to resolve any ambiguities, questions and other issues that may arise after and as a result of the interview. We also need to record your data to keep track of the interview process. The project's deliverables that will be derived by the interview will not include your personal data or any other information that could identify you. Your personal data will remain on our written notes (interview's transcript) and/or the sound recording we will make during the interview.

We will share your data with a few other RURALITIES project partners that are also involved in this task and will participate in the drafting of the relevant deliverables. We are also obliged to grant access to your data to:

- EU officials such as our Project Officer for purposes related to project's evaluation;

- EU agencies and other authorities for project's auditing purposes.

We would also be very happy if you gave us your consent to contact you in the future to ask you to participate in other project's activities (e.g., surveys, interviews, project events, RURALITIES Advisory Board, etc.) and also to inform you about the project's progress (e.g., by sending you a newsletter or similar messages).

How can you withdraw your consent?

You should know that you can withdraw your consent at any time by communicating either on the phone or by email with the responsible persons listed in the previous page. With regards to the informational messages and newsletters you can always opt out by simply clicking the link ''Unsubscribe'' or something similar included at the end of all the relevant messages.

I hereby give my consent to the processing of my personal data needed for:

*(Please, tick the boxes below to confirm that you give us your consent for the respective subject. Any boxes left unticked mean that **you do not consent to the relevant subject**.)*

#	Consent Subject	Tick box
1	My participation in an interview that will be carried out by RURALITIES to < insert key objective of the interview >	
2	My participation in future activities of RURALITIES	
3	Receiving newsletters and messages regarding RURALITIES activities	

_____   _____   _____

Name of participant   Date   Signature

Funded by the European Union

ANNEX 3 PRIVACY POLICY

In this Annex we include the Privacy Policy elaborated for the web page, which will be adapted and included in any interface requiring users to connect and introduced personal data.

Privacy & Cookies Policy

For RURALITIES website

1. Who we are

RURALITIES is a cross-national 5-year long Coordination and Support Action (01/10/2022- 30/09/2027), supported by the European Union within the framework of the Horizon Europe programme.

The project delivers an ecosystem-enhancing and climate action driven expertise and learning framework organized in hubs e.g., the 'RURALITIES', comprising a series of innovative methodologies with the learner at its core, supported by a comprehensive network of living labs, and a blockchain-based digital platform combining the Internet and wireless technologies, to assist engage, connect and empower actors.

Within the framework of RURALITIES project, accessible from https://www.ruralities-project.eu/ , one of our main priorities is the privacy of our visitors. This Privacy and Cookies Policy document contains types of information that is collected and recorded by RURALITIES project and how we use it. If you have additional questions or require more information about our Privacy and Cookies Policy, do not hesitate to contact us.

The partners of the RURALITIES consortium, listed below, process certain types of personal data for the purposes of the project. Each partner is responsible for the personal data they collect and process during their activities under the framework of the project:

	Participant organisation name	**Country**
1	PEDAL Consulting s.r.o.	Slovakia
2	Asociatia Rural Development Research Platform	Romania
3	Center For Technology Research and Innovatio Ltd	Cyprus
4	Asociacion De Investigacion De Industrias Carnicas Del Principado De Asturias	Spain
5	Kemijski Institut	Slovenia
6	Universidad Politecnica De Madrid	Spain
7	Institut Za Razvoj I Inovacije - Iri	Serbia
8	Particula Group Drustvo S Ogranicenom Odgovornosc u Za Istrazivanje Razvoj I Proizvodnju	Croatia
9	Sveuciliste U Zagrebu Agronomski Fakultet	Croatia
10	African Centre For Technology Studies	Kenya
11	Centro De Investigacao E Transferencia De Tecnologia Para Desenvolvime nto Comunitario	Mozambique
12	European Society For Quality And Patient Safety In General Practice/family Medicine	Denmark
13	Mugla Sitki Kocman University	Turkey

	Participant organisation name	Country
14	Marin Biyoteknoloji Urunleri Ve GidaSanayi Ticaret Limited Sirketi	Turkey
15	Université Libre de Bruxelles	Belgium
16	Inagro, Provinciaal Extern Verzelfstandigd Agentschap In Privaatrechteli jke Vorm Vzw	Belgium
17	Arab Academy For Science, Technology And Maritime Transport	Egypt
18	Regionalna razvojna agencija Posavje	Slovenia
19	Yxs Avalana S.r.l.	Romania
20	Universitatea Pentru Stiintele Vietii "Ion Ionescu De La Brad"	Romania
21	Asociatia Grupul De Actiune Locala Siret-Moldova	Romania
22	Sokoine University of Agriculture	Tanzania
23	Université de Nouakchott Al Aasriya	Mauritania
24	Institut Facultaire Des Sciencesagronomiques (Ifa) De Yangambi	D.R. Congo
25	Alternative Communautaire Pour Le Developpement Durable	Côte d'Ivoire
26	Prototipi Limited	Nigeria
27	Almanar Voluntary Organization	Sudan
28	Communication Pour Un Developpement Durable C.D.D.	Togo
29	Youths in Technology and Development Uganda Limited	Uganda
30	Fundacion Ctic Centro Tecnologico Para El Desarrollo En Asturias De Las Tecnologias De La Informacion	Spain
31	Fondazione Homo Viator - San Teobaldo	Italy
32	Montefeltro Sviluppo Società Consortile a Responsabilità Limitata	Italy
33	Museum Grafia	Italy
34	La Corte Della Miniera S.r.l.	Italy
35	Desarrollo De Estrategias Exteriores SA	Spain
36	Asociacion Red Asturiana De Desarrollo Rural	Spain
37	Montagna Vicentina Societa Cooperativa	Italy
38	Maroc Horizon D' Aventures	Morocco
39	University of Malawi	Malawi
40	0kmnomads.org	Ghana
41	Magyar Agrar- Es Elettudomanyi Egyetem	Hungary
42	Ecole Nationale d'Ingénieurs de Carthage	Tunisia
43	University Assane Seck of Ziguinchor	Senegal
44	Confederation Paysanne Du Faso	Burkina Faso
45	University of Rwanda	Rwanda
46	Zambia Land Alliance	Zambia
47	Evrosad Proizvodnja Trgovina Evetovanje D.O.O.	Slovenia
48	Turisticno Drustvo Senovo	Slovenia
49	Instituto D' Istruzione Superiore a. Cecchi	Italy
50	The Highlands And Islands Transport Partnership	UK

	Participant organisation name	Country
51	Aspire-igen Group Limited	UK
52	Conservation Education And Research Trust	UK

For further information, we can be contacted at: info@ruralities-project.eu

2. How we collect personal data?

We collect personal data both directly and indirectly:

Directly. We obtain personal data directly from individuals in a variety of ways, including but not limited to the following cases:

- an individual subscribes to our newsletter/s;
- an individual registers to attend meetings and events we host and during attendance at such events;
- we establish cooperative relationships with an individual;
- we provide professional services pursuant to our contract with the European Commission;
- an individual participates in an interview or survey organized by us.

Indirectly. We obtain personal data indirectly about individuals from a variety of sources, including:

- our research partners;
- our networks and contacts;
- public and open data sources such as public registers, news articles and internet searches;
- social and professional networking sites (e.g., LinkedIn).

3. What type of data we collect?

We only collect the data that are necessary for the smooth implementation of our project. These data fall into the following categories:

- contact details (name/ surname, e-mail address, street address, mobile phone number, land line phone number);
- professional information (job title, organization, field of expertise);
- demographics (e.g., age, gender, nationality);
- information about what a person knows or believes.
- videos and photos (from people that attend our events).

4. Basis of lawful processes

We process personal data on the following legal bases:

Legal obligations – for processing activities required for compliance both with applicable national and European legislation as well as with the specific legal and regulatory framework of the Horizon Europe Framework Programme for Research and Innovation of the European Union.

Consent – for processing activities such as organization of surveys and interviews, completing of questionnaires and dissemination of project's results.

Contractual obligations – for processing activities such as reporting to the European Commission and complying with project's publicity obligations.

5. What we do with your personal data?

We process your personal data with the purpose of:

- Conducting research (e.g., interviews, surveys);
- Dissemination our project's results to different types of stakeholder;
- Sending invitations and providing access to guests attending our events and webinars;
- Administering, maintaining, and ensuring the security of our information systems, applications, and websites;
- Processing online requests or queries, including responding to communications from individuals;
- Complying with contractual, legal, and regulatory obligations.

6. How we secure your personal data when we process it?

We continuously apply a personal data risk assessment process to identify, analyze, and evaluate the security risks that may threat your personal data. Based on the results of this risk assessment, we define and apply a set of both technical and organizational measures to mitigate the above security risks, including but not limited to:

- Data Protection Policies to guide our personnel when processing your data;
- Written contracts with organizations that process personal data on our behalf;
- Non-Disclosure Agreements with our personnel;
- Back up process, antimalware protection, access control mechanisms, etc.
- Some of our partners have appointed a Data Protection Officer.

7. Do we share personal data with third parties?

We may occasionally share personal data with trusted third parties to help us deliver efficient and quality services. When we do so, we ensure that recipients are contractually bound to safeguard the data we entrust to them before we share the data. We may engage with several or all the following categories of recipients:

- Parties that support us as we provide our services (e.g., cloud-based software services such as Dropbox, Microsoft SharePoint, Google);
- Our professional advisers, including lawyers, auditors, and insurers;
- Dissemination services providers (e.g., MailChimp);
- Law enforcement or other government and regulatory agencies or other third parties as required by, and in accordance with applicable law or regulation;
- The European Commission according to our relevant contractual obligations.

RURALITIES project's Privacy Policy does not apply to other advertisers or websites. Thus, we are advising you to consult the respective Privacy Policies of these third-party ad servers for more detailed information. It may include their practices and instructions about how to opt-out of certain options. You can choose to disable cookies through your individual browser options. To know more detailed information about cookie management with specific web browsers, it can be found at the browsers' respective websites.

8. Do we transfer your personal data outside the European Economic Area?

We do not own file servers located outside the European Economic Area (EEA). However, some partners may use cloud and / or marketing services from reputable providers such as SharePoint, DropBox, MailChimp, Google, etc., situated both inside and outside the EEA. We always check that such providers comply with the relevant GDPR requirements before start using their services.

9.   General Data Protection Regulation (GDPR)

We are a Data Controller of your information and will retain your personal information only for as long as it is necessary for the purposes set out in this Privacy Policy. We will retain and use your information to the extent necessary to comply with our legal obligations, resolve disputes, and enforce our policies. If you are a resident of the European Economic Area (EEA), you have certain data protection rights. If you wish to be informed what Personal Information we hold about you and if you want it to be removed from our systems, please contact us. In certain circumstances, you have the following data protection rights:

- The right to access, update or to delete the information we have on you
- The right of rectification
- The right to object
- The right of restriction
- The right to data portability
- The right to withdraw consent

10. Log files

RURALITIES project follows a standard procedure of using log files. These files log visitors when they visit websites. All hosting companies do this and a part of hosting services' analytics. The information collected by log files include internet protocol (IP) addresses, browser type, Internet Service Provider (ISP), date and time stamp, referring/exit pages, and possibly the number of clicks. These are not linked to any information that is personally identifiable. The purpose of the information is for analysing trends, administering the site, tracking users' movement on the website, and gathering demographic information.

11. Privacy Policies

You may consult this list to find the Privacy Policy for each of the advertising partners of RURALITIES project. Third-party ad servers or ad networks uses technologies like cookies, JavaScript, or Web Beacons that are used in their respective advertisements and links that appear on RURALITIES project, which are sent directly to users' browser. They automatically receive your IP address when this occurs. These technologies are used to measure the effectiveness of their advertising campaigns and/or to personalize the advertising content that you see on websites that you visit. Note that RURALITIES project has no access to or control over these cookies that are used by third-party advertisers.

12. Children information

Another part of our priority is adding protection for children while using the internet. We encourage parents and guardians to observe, participate in, and/or monitor and guide their online activity. RURALITIES project does not knowingly collect any Personal Identifiable Information from children under the age of 13. If you think that your child provided this kind of information on our website, we strongly encourage you to contact us immediately and we will do our best efforts to promptly remove such information from our records.

13. Online Privacy Policy Only

Our Privacy Policy applies only to our online activities and is valid for visitors to our website with regards to the information that they shared and/or collect in RURALITIES project. This policy is not applicable to any information collected offline or via channels other than this website.

14. Do we use cookies?

Our websites use cookies. Where cookies are used, a statement will be sent to your browser explaining the use of cookies. To learn more, please refer to our cookie policy.

Cookies are small text files which are saved on your computer, mobile phone or tablet. They allow the website to remember your actions and preferences (such as login, language, font size and other display preferences) so you don't have to keep re-entering them whenever you come back to the site. You can control and/ or delete cookies as you wish. If you do this, however, you may need to manually adjust your preferences every time you visit a site. For more information on how to manage cookies, please visit: http://www.aboutcookies.org/

We use tools like Google Analytics to better understand how visitors interact with our website. This provides us with important information to enable the site to work better. The information collected is not linked to your personal data. For more information on the cookies set by Google Analytics, please visit: http://code.google.com/apis/analytics/docs/concepts/gaConceptsCookies.html

The following cookies are necessary and are always enabled:

Name	Typical content	Cookie expires after
__cf_bm	The cookie is set by cloudflare. This cookie is used to distinguish between humans and bots. This is beneficial for the website, in order to make valid reports on the use of their website.	30 minutes
cookielawinfo-checkbox-analytics	This cookie is set by GDPR Cookie Consent plugin. The cookie is used to store the user consent for the cookies in the category "Analytics".	11 months
cookielawinfo-checkbox-functional	The cookie is set by GDPR cookie consent to record the user consent for the cookies in the category "Functional".	11 months
cookielawinfo-checkbox-necessary	This cookie is set by GDPR Cookie Consent plugin. The cookies is used to store the user consent for the cookies in the category "Necessary".	11 months
CookieLawInfoConsent	This cookie is set by GDPR Cookie Consent plugin. The cookie records the default button state of the corresponding category along with the status of CCPA.	11 months
viewed_cookie_policy	The cookie is set by the GDPR Cookie Consent plugin and is used to store whether or not user has consented to the use of cookies. It does not store any personal data.	11 months

The following cookies are for analytics and are optional:

Name	Typical content	Cookie expires after

_ga_*	This cookie is set by Google Analytics. This cookie is used to store and count pageviews.	2 years
_gat	Used to throttle request rate	1 minute
_ga	This cookie is set by Google Analytics. This cookie is used to distinguish users.	2 years

15. Consent

By using our website, you hereby consent to our Privacy Policy and agree to its terms.

ANNEX 4 DATA SUBJECT REQUEST FORM

This Annex contains the Data subject request form, that is used to submit a data subject request under the provisions of the European Union General Data Protection Regulation (GDPR).

Text in red color contains guidelines for adjusting this template and should be deleted.

Text included in < > and/or highlighted with grey should be replaced with content that is suitable to the context of each activity & project as well as to the organization seeking to obtain the consent.

RURALITIES

Data Subject Request Form

You may delete the data referring to the Data Protection Officer if your organisation does not have one.

Contact

<Insert name of responsible Project Manager>   <Insert name of DPO > **(Data Protection Officer)**

<Insert email of responsible Project Manager>   <Insert e-mail of DPO >

Data Subject Request Form

This form should be used to submit a data subject request under the provisions of the European Union General Data Protection Regulation (GDPR).

Submitter Details

Title:	
Name:	
Address:	

Type of Request

Please select the type of request you are making:

☐   *Consent Withdrawal*

☐   *Access request*

☐   *Rectification of personal data*

☐   *Erasure of personal data*

☐   *Restriction of processing of personal data*

☐   *Personal data portability request*

☐   *Objection to processing of personal data*

☐   *Request regarding automated decision making and profiling*

Personal data involved

Request details

Request reason/justification

Name: ……………………………………………………………………………….

Signature: ………………………………………………

Date: ……………………………………………………

<center>***</center>

Once completed, this form should be submitted via e-mail to < Insert contact e-mail of Partner > or posted to:

< Insert Partner Name >

< Insert Partner Address >