SOlutions **TE**sting for **R**egions through

Insurance for Climate **A**daptation

HORIZON-MISS-2022-CLIMA-01| Project Number 101112867

Deliverable 5.2

Data Management Plan

Due date of deliverable: 29/02/2024

Actual date of submission: 21/02/2023

Start date of project: 1st September 2023
Duration: 30 months
Beneficiary responsible for the Deliverable: SINTEF

Dissemination Level		
PU	Public	**x**
SEN	Sensitive — limited under the conditions of the Grant Agreement	
CI	EU classified, as referred to in Commission Decision 2001/844/EC	

* PU: Public — fully open. SEN: 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. For items classified under other rules (e.g. national or international organization), please select the equivalent EU classification level.

List of **Contributors**

Organization	Name	Contribution
SINTEF	Luis Caetano, Eli Sandberg	Authors
BC3	Laura Vay	Reviewer

Modification **Control**

Version	Date	Description & Comments	Responsible
0.1	30/01/2024	First draft	SINTEF
0.2	05/02/2024	Updated based on reviewers' comments.	SINTEF
0.3	12/02/2023	Updated based on reviewers' comments.	SINTEF
Final	20/02/2024	Final document	Coordinator

General **Project Information**

Title	SOlutions TEsting for Regions through Insurance for climate Adaptation
Acronym	SOTERIA
Grant Agreement No.	101112867
Funding Programme	HORIZON EUROPE
Topic	HORIZON-MISS-2022-CLIMA-01-03
Type of action	HORIZON Research and Innovation Actions
Project Start Date	1st September 2023
Duration of the project	30 Months

List of **SOTERIA** Partners

№	ORGANISATION	Short name	Country	Role
1	Basque Centre for Climate Change	BC3	ES	Coordinator
2	I-Catalist SL	ICA	ES	Beneficiary
3	Climate Risk Advisory Ltd	CRA	NO	Beneficiary
4	Helmholtz Centre for Environmental Research	UFZ	DE	Beneficiary
5	SINTEF AS	SINTEF	NO	Beneficiary
6	Mitigrate AS	MITI	NO	Beneficiary
7	AQUATEC	AQUA	ES	Beneficiary
8	Genillard & Co GmbH	G&Co	DE	Beneficiary
9	National Center for Scientific Research Demokritos	DEMO	GR	Beneficiary
10	Hochschule Weihenstephan-Triesdorf	HSWT	DE	Beneficiary
11	Association for the Development of West Athens	ASDA	GR	Beneficiary
12	Behavior SMART OOD	BES	BG	Beneficiary
13	Generalitat Valenciana	GVA-A	ES	Beneficiary
14	Municipality of Gabrovo	MoG	BG	Beneficiary
15	Empower Insight	EI	FR	Beneficiary
16	Stiftung Global Infrastructure Basel	GIB	CH	Associated Partner
17	Verbraucherzentrale Sachsen e.V.	VZS	DE	Associated Partner
18	Landesamt für Umweltschutz (Regional Env. Protection Agency)	LAU	DE	Associated Partner
19	KLP Skadeforsikring AS (insurance)	KLP-S	NO	Associated Partner
20	Gjensidige Forsikring ASA (insurance)	GJE	NO	Associated Partner
21	Allianz Agrar (insurance)	AZA	DE	Associated Partner
22	Croatia Osiguranje (insurance)	CO	HR	Associated Partner
23	German Insurance Association	GDV	DE	Associated Partner
24	DIMOS EGALEO (insurance)	EGL	GR	Associated Partner
25	Bavarian Farmers Association	BBV	DE	Associated Partner
26	Zadar County, Croatia	ZDC	HR	Associated Partner
27	The County Governor in Trøndelag	CGT	NO	Associated Partner
28	DZI at KBC Group (insurance)	DZI	BG	Associated Partner
29	Caisse de Reassurance (insurance)	CCR	FR	Associated Partner
30	Ethniki AEEGA (insurance)	Ethniki	GR	Associated Partner

Executive Summary

The SOTERIA project aims to advance innovative insurance solutions for Climate Change Adaptation in different European regions and communities. SOTERIA will take these solutions from the levels of research to demonstration and testing with some at the level of pre-commercial procurement in at least three cases. This way SOTERIA will contribute to the wider goal of the Mission Adaptation to increase Europe's resilience and preparedness to face unavoidable consequences of climate change by filling the gaps on insurance coverage for climate change adaptation.

This deliverable contains the data management plan (DMP) that describes the data management lifecycle for data that is acquired, processed and/or generated by the SOTERIA project. The DMP ensures good and safe handling of data throughout the research process, the best quality data, and that data lives on and can be reused after the end of the project. DMP addresses compliance with any ethical and data protection requirements.

This document will be reviewed and updated in Nov.2024 and a final version should be delivered in Feb.2026.

Index

Abbreviations

BibTeX	A reference management software for formatting lists of references.
CC licence	Creative Commons licenses are tools to grant copyright permissions to creative work.
CC-BY	This CC-license lets others distribute, remix, tweak, and build upon your work, even commercially, if they credit you for the original creation. This is the most accommodating of licenses offered. Recommended for maximum dissemination and use of licensed materials.
CC-BY-NC	This CC-license lets others remix, tweak, and build upon your work non-commercially, and although their new work must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.
CC-BY-SA	This CC-license lets others remix, tweak, and build upon your work even for commercial purposes, if they credit you and license their new creations under the identical terms. This license is often compared to "copyleft" free and open-source software licenses. All new works based on yours will carry the same license, so any derivatives will also allow commercial use.
CSL	Citation Style Language An open XML-based standard to format citations and bibliographies.
DMP	Data Management Plan
DoA	Description of the Action
DOI	Digital Object Identifier
FAIR data	Findable, Accessible, Interoperable, Re-usable data
GDPR	General Data Protection Regulation. Regulation (EU) 2016/679.
JSON	JavaScript Object Notation An open-standard file format.
MARCXML	An XML schema based on the common MARC21 standards.
OAI-PHM	The Open Archives Initiative Protocol for Metadata Harvesting.
Research data	Refers to information, facts or numbers, collected to be examined and considered as a basis for reasoning, discussion, or calculation. In a research context, examples of data include statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings, and images.
REST API	REST is an architectural style that defines a set of constraints to be used for creating web services. API means Application Programming Interface.
SSL/TLS	Secure Sockets Layer / Transport Layer Security These are protocols offering secure communication on the internet.
Zenodo	Zenodo is a catch-all research data repository that enables researchers, scientists, EU projects and institutions to share research results, make research results citable, and search and reuse open research results from other projects. Zenodo is harvested by the OpenAIRE portal and hosted by the CERN cloud infrastructure.

1. Introduction

Purpose of the document

The purpose of the DMP is to contribute to good data handling through describing what research data the project expects to generate and which parts of the data that can be shared with the public. Furthermore, it gives instructions on naming conventions, metadata structure, storing of the research data and how to make public data available. During the 30 active months of the project, a GoogleDrive site will be used as the online working and collaboration platform. GoogleDrive is only accessible to project participants and can provide further access control through establishing folders and sub-sites with stricter access granted than to the main site. All datasets will be uploaded to this site and stored and handled in accordance with the specific agreement with the data owner (when applicable), and national and European rules on data protection and privacy. Metadata will be added to all datasets, and instructions on how to upload and store research data is provided in this document.

SOTERIA will use the open research data repository Zenodo to comply with the Horizon Europe Open Access Mandate. This mandate applies to the underlying research data of publications, but beneficiaries can also voluntarily make other datasets open. In SOTERIA, all public deliverables and publications including related research data will be uploaded to the SOTERIA Community and the European Commission Funded Research (OpenAIRE) Community in Zenodo. Other datasets not directly linked to deliverables and publications that has the dissemination level "Public" will also be uploaded to Zenodo. Uploads will be done upon approval of the deliverables by the European Commission, upon publication or acceptance of scientific publications, or, for underlying datasets, at the end of the project at the latest. Each dataset will be given a persistent identifier (Digital Object Identifier, DOI), supplied with relevant metadata, and linked to the project name and grant agreement number. Publications and underlying research data will be linked to a Creative Commons license that will regulate reuse of the SOTERIA research data. Data security arrangements are defined for the Google Drive site and Zenodo.

Ethical aspects related to data collection, generation and sharing have been considered and nothing in this project shall be deemed to require a party to breach any mandatory statutory law under which the party is operating. This includes any national or European regulations, as well as rules and norms regarding ethics in conducting research. The DMP is a living document and will be updated throughout the project to reflect the actual research data generated. The final version of the DMP will be made available at the end of the project and include instructions for how to access and reuse open research data from SOTERIA. Day-to-day data management and monitoring will be done using an online list in the Google Drive site that will be continuously updated to reflect actual data generation.

Intended readership

Internally in the project:

- Project participants who are responsible for, or in any way involved with, data collection and data handling can use this document for instructions on how to handle, store and process data.
- All project participants can use this document to get an overview of data collected in the project and how this is processed, stored and made accessible.

External audience:

- The Data Summary and FAIR Data Management sections can be used by all relevant stakeholders

who are interested in SOTERIA related activities and research topics to get an overview of the data collected in the project, how to access this data, and, if applicable, how to re-use this data in their own activities.

Structure of this document

This document is structured as follows:

- Section 1 is an introduction chapter describing the main purpose, structure and intended readership of the DMP, as well as relationships to other project deliverables.
- Section 2 provides an overview of the research data in the SOTERIA project, with details on types, formats, origin and metadata provisions.
- Section 3 describes how the SOTERIA project will comply with the principles of FAIR data management and Horizon Europe Open Access Mandate.
- Section 4 describes the resources allocated to making data FAIR and open.
- Section 5 gives a detailed description of data security arrangements.
- Section 6 deals with ethical aspects related to data management in the SOTERIA project.

The online tool DMPOnline, hosted by Data Curation Centre, has been used to generate content for this document[1]. The tool is based on the Horizon Europe DMP template and guidelines for FAIR data.

2. Data Summary

Table 2, on page 16, provides a list of all datasets currently expected to be generated in the SOTERIA project and their planned accessibility. We recognise that this list will develop and grow as the project evolves.

Purpose of the data collection

The overall motivation for data collection in SOTERIA is to understand how to make regions involved in the project more resilient and better adapted through better use of data.

Only data that is needed to perform project activities will be collected, and as far as possible, participants will not be asked to provide personal data unless this is necessary.

Data types, formats and size

The data collected in the SOTERIA project will include climate-related risk and loss data from insurance companies and public data needed for risk assessment (map data for buildings, infrastructure and other land use, terrain data, vegetation, ground conditions, etc.). The insurance loss data is competition sensitive and may contain personal information (such as addresses). Informed consent forms should be distributed to the owners of loss data to clarify if loss data is planned to be shared and published within the project in anonymised and aggregated level.

[1] https://dmponline.dcc.ac.uk/about_us

The SOTERIA project will collect, generate and reuse various data sources, such as:

- Manually collected data from interviews, surveys, and questionnaires.
- Loss data from insurance companies.
- Contact information (e.g. project internal and external stakeholders/participants in pilots/workshops/evaluation activities etc.).
- Existing climate-related risk data from literature reviews, databases or statistics.
- Calculation data (data from models, simulations, and other calculations).

Data will be organised in datasets according to type and content of the data.

Some of the data SOTERIA will collect and generate may be classified as *personal data*, as defined by GDPR including names, addresses, location, etc.. This data must be irreversibly anonymised before being made public. If such data cannot be irreversibly anonymised, it will remain confidential and only managed by designated Data Controllers in the project. If a partner who is not a Data Controller needs access to process personal data (Data Processer), an assessment of this will be done by the Data Controller and if granted a specific Data Processing Agreement will be set up between the Data Controller and the partner requesting access. A template for Data Processing Agreement is provided in appendix A. Non-anonymous data, although not openly shared in the project or beyond, can still provide input to deliverables and publications. Only non-market sensitive data, anonymised data or analysis of the aggregated data, containing no details that can be linked to individual participants, will be made public.

Data formats

The SOTERIA project will only use widely accepted formats for data generation, such as:

- **Documents/Reports/Publications:** .PDF/A, txt, doc/docx
- **Spreadsheets:** .xls/.xslx
- **Databases:** .csv
- **Audio files:** .mp3, .wav, .wma, .ra
- **Pictures:** jpg, png
- **Video:** avi, flv, mov, mp4, wmv

A dataset can include different types of formats. As an example, a manually collected dataset concerning user acceptance can consist of both written interview notes, audio files from interviews, pictures from pilot sites, and survey responses. Some of this data cannot be anonymised within the scope of this project (e.g. audio files, interview transcripts in local languages), so in most cases only parts of a dataset can be made openly available.

Size of data

The size of the data will vary but will in general be moderate and should not represent any challenge regarding storage capacity or handling. A more detailed list of planned datasets and accessibility is given in Table 2.

Origin of data

The SOTERIA project will collect data at 7 locations: Leipzig/Saxony, Bavaria, Trøndelag, Valencia, West Athens, Gabrovo and Zadar. Depending on the type of data, there will be various methods and origins of data collection involved at each site.

For manually collected data the main origins will be:

- Interviews with groups and individual participants in the pilots/demonstrations/etc. at each site. [2]
- Feedback from participants at stakeholder workshops.
- Survey responses.
- Market survey.
- Literature study/review and open research data (re-use of existing data).

For automatically collected data the main origins will be:

- Automated data collection using scripts.

Data validation

Before releasing datasets to the public, it's essential to undergo a validation process. The data validation process should ensure the accuracy, reliability, and integrity of the data collected and processed during the project. The validation process could include automated checks for data format and consistency, manual reviews for data quality, or specific validation techniques relevant to the data types and sources used in the project.

GoogleDrive

All datasets in the SOTERIA project will be stored in a BC3 GoogleDrive project site. This will be the projects online collaboration area during 30 months the project is active. All partners will be responsible for uploading the datasets they have collected/generated during the project. Each dataset will be catalogued in a list providing an overview of all datasets in the project, as well as uploaded to a dedicated research data folder in the GoogleDrive site. All datasets will use standard GoogleDrive version control and access control is available to enable limited access to certain types of data.

Zenodo

SOTERIA will use Zenodo, a trusted and OpenAire compliant repository to comply with the FAIR principles. All scientific publications, including public deliverables and public parts of underlying datasets will be uploaded to the SOTERIA Community. In addition, the project will upload other datasets (not directly linked to publications and deliverables) with dissemination level "Public" and make them openly accessible via the repository.

Naming conventions

Data will be named using the following naming conventions:

Descriptive text_HEU_Acronym_DeliverableNumber_UniqueDataNumber

Descriptive text_HEU_Acronym_PublicationNumber_UniqueDataNumber

Explanation of the naming convention:

[2] To ensure uniformity, the following interview documents should be uploaded to their respective project folders: 1. transcriptions in txt format, 2. the original audio files, and 3. photographs, among others.

- "Descriptive text" refers to a *short* description of the content of the dataset (see example)
- "Acronym" refers to the project's short name or acronym; SOTERIA
- "DeliverableNumber" refers to the deliverable number as described in the DoA
- "PublicationNumber" refers to the number the publication has in the project internal directory of all publications from the project

Example of dataset name:

APP user acceptance_ HEU_SOTERIA_D1.1_003

Weather data OSL Jan 2019_HEU_SOTERIA_07_017

Instructions for uploading data to GoogleDrive

Table 1 and Figure 1 provide instructions to project participants on how to upload data to GoogleDrive and Zenodo:

Table 1: Instructions for uploading data to GoogleDrive

Upload instructions - SOTERIA GoogleDrive Site

• Please upload all SOTERIA data listed in Table 2to this folder in the SOTERIA GoogleDrive site:
  ○ *SOTERIA Drive: SOTERIA Datasets*
• Use this naming convention (for details see 2.1.2):
  ○ *Descriptive text HEU_Acronym_DeliverableNumber_UniqueDataNumber*
  ○ *Descriptive text HEU_Acronym_PublicationNumber_UniqueDataNumber*
• Be sure to use the same file name when uploading later versions

Upload instructions - Zenodo

• Research data underlying scientific publications/classified as "Public" should, in addition, be uploaded to the SOTERIA Community in Zenodo. To do this you must complete the following steps:
  ○ Create a profile in Zenodo to be able to upload files.
  ○ Click on the *SOTERIA Community* link above, or search for " *SOTERIA Community*" under the "Communities" tab at the top of the Zenodo site.
  ○ On the Community site, click the green "New upload" button in the top right corner
  ○ Enter requested data and confirm the upload.
  ○ Remember to add the European Commission community in the box labelled "communities". You can use the search function to locate the community and add it. The data will then automatically be uploaded to both communities, so you do not have to do it twice.
• Uploading should be done as soon as possible and at the latest on article publication or EC approval of deliverables for underlying datasets. Other datasets will be uploaded in the final month of the project at the latest.
• Each partner is responsible for uploading data sets collected/generated by them. If needed, task leader in WP2 will supply assistance.

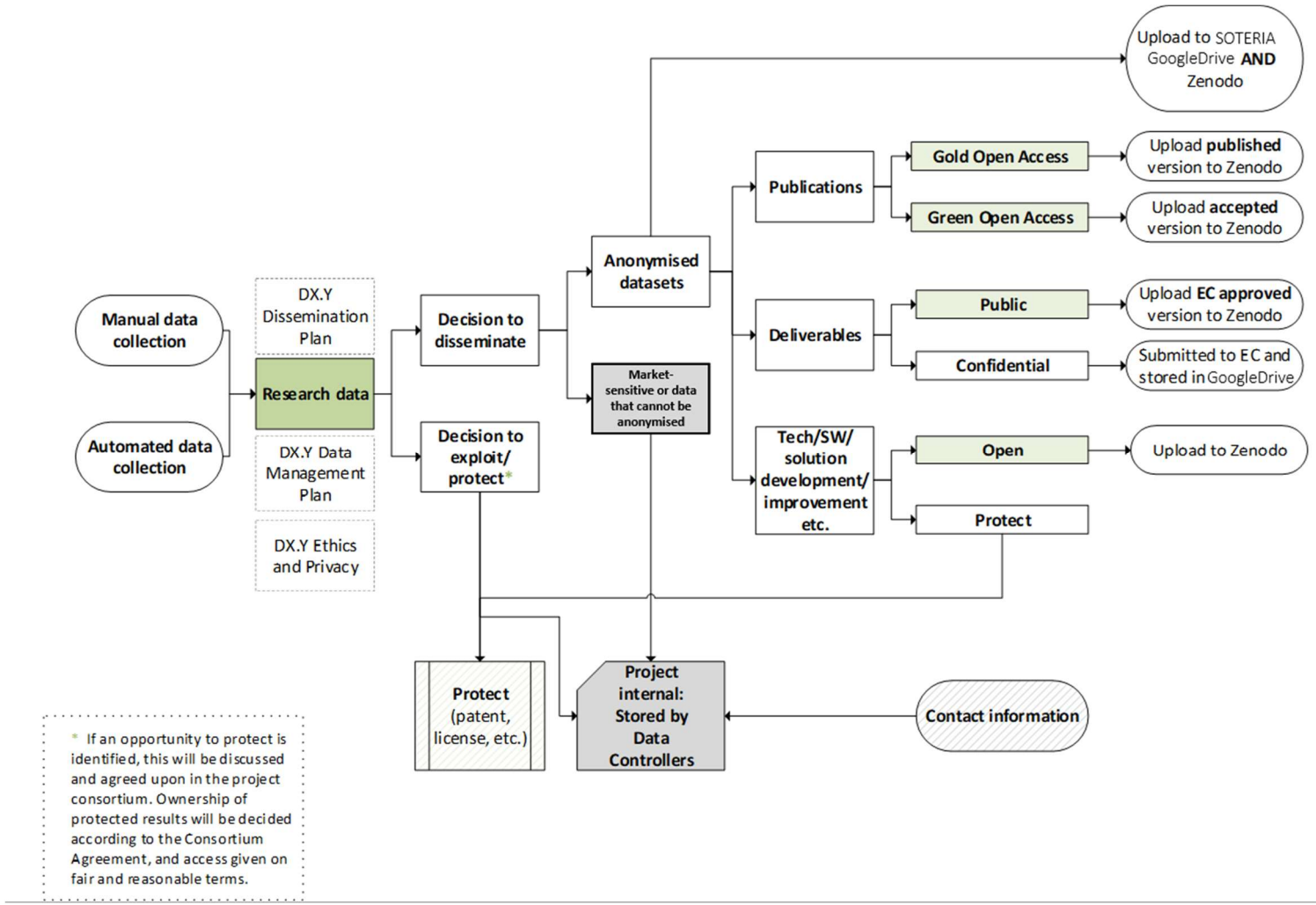

Figure 1: Process for uploading datasets.

3. FAIR Data Management

SOTERIA will manage data in accordance with the principles of **FAIR data management**[3] (Findable, Accessible, Interoperable and Re-usable data). The project aims to maximise access to, and re-use of research data generated by the project. At the same time, there are datasets, or parts of datasets, generated in this project that cannot be shared in order to protect the privacy of voluntary participants in the pilots or to protect business sensitive information. Table 2 provides a current overview of the expected datasets in the SOTERIA project and their accessibility.

Making data findable

SOTERIA Community in Zenodo

SOTERIA will use the Zenodo repository as the main tool to make our research data findable in accordance with the Horizon Europe Open Access Mandate.

A *SOTERIA* community has been established in the Zenodo repository, and the project will upload all our public datasets and deliverables as well as scientific publications to this community. In addition, we will link all our uploads to the *European Commision Funded Research (OpenAIRE)* community for maximum findability. All uploads will be enriched with standard Zenodo metadata, including Grant Number and Project Acronym. Zenodo provides version control and assigns DOIs to all uploaded elements.

Metadata in Zenodo

Metadata associated with each published data set in Zenodo will by default be as follows:

- Digital Object Identifiers
- Version numbers
- Creator (Name and ORCID)
- Keywords
- Abstract/description
- Associated project and community
- Associated publications and reports
- Grant information
- Access and licensing info
- Language

In addition, we will add the project name and GA number.

Versioning and Digital Object Identifiers (DOI)

Zenodo provides DOI versioning of all datasets uploaded to their communities, which allows us to edit and update the uploaded datasets after they have been published. This also allows us to cite specific versions of an upload and cite all versions of an upload. As an example, DOI versioning of an uploaded software package that is released in two versions can look like this[4]:

[3] http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-data-mgt_en.pdf
[4] http://help.zenodo.org/ (DOI versioning)

- v1.0 (specific version): 10.5281/zenodo.60943
- v1.1 (specific version): 10.5281/zenodo.800648
- Concept (all versions): 10.5281/zenodo.705645

The first two DOIs for versions v1.0 and v.1.1 represent the specific versions of the software. The last DOI represents all the versions of the given software package, i.e. the concept of the software package and the ensemble of versions. They are therefore also referred to as *Version DOIs* and *Concept DOIs*, but technically they are both normal DOIs.

This does not, however, mean that you will receive a new DOI each time you edit the metadata related to your upload (e.g. change the title of a file or dataset). A new DOI version will only be created if you update the actual files you have uploaded.

Approach to search keywords

Each partner who collects and generates public datasets will be responsible for uploading these to Zenodo and to assign specific search keywords relevant to these datasets. Dataset specific keywords must be descriptive to the content of the dataset. E.g., a dataset containing information on user acceptance of a solution should be tagged with corresponding keywords such as, "*Solution"/"user acceptance*". In addition, the project has defined a set of general keywords that apply to all public datasets, scientific publications and public deliverables. These are as follows:

- Climate change adaptation
- Insurance & Finance

Making data accessible

The Horizon Europe Open Access Mandate aims to make research data generated by Horizon Europe projects accessible with as few restrictions as possible, but also accept protection of personal or sensitive data due to privacy concerns and/or commercial or security reasons.

All public datasets, scientific publications and deliverables will be uploaded to Zenodo and made openly available, free of charge. Publications and underlaying data sets will be linked through use of persistent identifiers (DOI versioning). Data sets with dissemination level "confidential" (non-anonymous datasets) will not be shared due to privacy/security/ethical concerns. Potentially, some datasets might be restricted due to protection for commercial exploitation. If such cases arise during the project, this will be informed in the final version of the DMP. Metadata including licences for individual data records as well as record collections will be harvestable using the OAI-PHM protocol by the record identifier and the collection name. Metadata is also retrievable through the public REST API. The data will be available through www.zenodo.org, and hence accessible using any web browsing application. No specific software or hardware is needed to access and reuse the data.

Table 2 below provides a list of all datasets expected to be generated in the SOTERIA project and their planned accessibility. This list constitutes the first version of dataset description and we recognise that it will develop and grow as the project evolves. In addition, some information concerning the datasets currently remain unknown, e.g. size of the datasets. An updated version of the list containing all dataset details will be provided at the end of the project.

Table 2: Expected datasets in SOTERIA

WP	Task	Name of dataset	Description/Purpose	Format	Responsible	Type	Diss. level	Comments
1	1.1	Pilot Story Maps	Characterisation of our pilots, as well as a replicable method to characterise other follow up regions	PDF, Excel	BS	DEM	CO	Confidential, only for members of the consortium (including the Commission Services)
1	1.2	Recommendations for regional data integration into the Risk Data Hub and vice versa	List of best practice recommendation for regional risk data hubs	PDF	CRA	R	PU	Subject to approval from coordinator
1	1.4	Co-design Innovation wheel of IIS	Interactive Insurance innovation wheel of examples of innovative solutions and replication guide for regions	PDF	MITI	DEC	CO	Confidential, only for members of the consortium (including the Commission Services)
1	1.5	Communities of Practice Diaries	Documentation of regional capacity building through IIS	PDF	ICA	R	CO	Confidential, only for members of the consortium (including the Commission Services)
2	2.2	Guidance on Best practices for data recording, collecting, storing and sharing	Best practice guidance (and templates) for regional data	PDF	SINTEF	R	PU	Subject to approval from coordinator
2	2.3	Tech Briefing on Data Drivers and barriers	Report on barriers and drivers for data for data recording, collection, storing and sharing climate-related risk and loss	PDF	SINTEF	R	PU	Subject to approval from coordinator

			data					
2	2.4	Guidelines on loss data	Guidelines for recording, collecting, storing and sharing climate-related loss data	PDF	SINTEF	R	PU	Subject to approval from coordinator
2	2.5	Source code for software prototype	Software prototype for use of climate-related risk and loss data	Source code	SINTEF	OTHER	PU	Subject to approval from coordinator
3	3.2	Guidelines on Best practices of insurance pricing and innovative insurance solutions	Mapping of existing and new innovative insurance products as well as best practise of pricing and costing methods.	PDF	G&Co	R	PU	Subject to approval from coordinator
3	3.2	Policy Rec on Sustainable Insurance – principles and rules	Mapping of the rules, principles, and metrics existing and PSI metrics, rules and principles (updated during the project lifespan) to feed into WP1	PDF	HSWT	R	PU	Subject to approval from coordinator
3	3.3	Radar of Success Stories of best practice insurance solutions and financial risk transfer mechanisms	Annual reports on latest developments in the field for our stakeholders in the pilots (“core group”), tool of communication	PDF	UFZ	R, DEC	CO	Confidential, only for members of the consortium (including the Commission Services)
3	3.4	Exploitation plan and SOTERIA strategy of market watch	Supporting questionnaire surveys, expert interviews, meta-studies for Climate Resilience dialogues in WP1/WP4 and our stakeholders in the pilots	.doc	UFZ	DEC	CO	Confidential, only for members of the consortium (including the Commission Services)

			("core group")					
3	3.5	Guidance on insurance pricing, product and services: Best practices and emerging insurance solution	Blueprint and learnings from pilots for innovative risk transfer solutions incl. design of ideal insurance product pricing methods for the SuperDeliverable of SOTERIA	PDF	G&Co	R	PU	Subject to approval from coordinator
4	4.1	Policy recommendations for affordable insurance cover	Extensive assessment of innovative insurance driven adaptation pathways amalgamating local surveys and stakeholders' knowledge	PDF	DEMO	R	PU	Subject to approval from coordinator
4	4.2	Climate Resilience Dialogue Series	A set of refined questions that will frame the dialogues with the regions and communities happening in WP1	.doc	GIB	DEC	PU	Subject to approval from coordinator
4	4.3	Policy Briefing Series on policy enabling framework	Main elements in the enabling framework for the adoption of IIS	PDF	BC3	R	PU	Subject to approval from coordinator
4	4.4	SuperDeliverable Best practice catalogue and Replication Manual for EU regions and communities	Final SuperDeliverable that collects all knowledge gathered	PDF	ICA	R	PU	Subject to approval from coordinator
		Consortium Agreement and Project Management Handbook	Deliverables for the internal functioning of the consortia	PDF	BC3	R	PU	Subject to approval from coordinator
5	5.1	SOTERIA periodic reporting to	Periodic report to the EU	PDF	BC3	R	PU	Subject to approval from

		EC						coordinator
5	5.4	Data management plan setting and periodical updating	Describing how to handle the research data	PDF	SINTEF	DMP	PU	Subject to approval from coordinator
5	5.3	IPR and Innovation Management – screening and periodical updating	Information on the IPR of the protect (as basis for exploitation)	PDF	UFZ	R	CO	Confidential, only for members of the consortium (including the Commission Services)
5	5.5	Dissemination and communication activities plan and reporting	D&C Plan (regularly updated)	PDF	EI	R	PU	Subject to approval from coordinator

R = Document, report (excluding the periodic and final reports); DEM = Demonstrator, pilot, prototype, plan designs; DEC = Websites, patents filing, press & media actions, videos, etc.; OTHER = Software, technical diagram, etc.

PU = Public, fully open, e.g. web; CO = Confidential, restricted under conditions set out in Model Grant Agreement;

Making data interoperable

Zenodo uses JSON schema as the internal representation of metadata and offers export to other formats such as Dublin Core, MARCXML, BibTeX, CSL, DataCite and export to Mendeley. The data record metadata will utilise the vocabularies applied by Zenodo. For certain terms, these refer to open, external vocabularies, e.g.: license (Open Definition), funders (FundRef) and grants (OpenAIRE). Reference to any external metadata is done with a resolvable URL.

Reusable data

The SOTERIA project will enable third parties to access, mine, exploit, reproduce and disseminate (free of charge for any user) all public data sets, and regulate this by using Creative Commons Licences.

Recommended Creative Commons (CC) licences

SOTERIA will use Creative Commons licences (CC), which are tools to grant copyright permissions to creative work. As a default, the CC-BY-SA license will be applied for public SOTERIA research data. This license lets others remix, tweak, and build upon your work even for commercial purposes, if they credit you and license their new creations under the identical terms. This license is often compared to "copyleft", free and open-source software licenses. With this licence all new work based on SOTERIA data and results will carry the same license, so any derivatives will also allow commercial use. This does not preclude the use of less restrictive licenses as CC-BY or more restrictive licenses as CC-BY-NC, which does not allow commercial usage.

Application of licences will be assessed on a case-by-basis in close collaboration with the coordinator, and partners concerned.

Availability and longevity of the SOTERIA research data sets

Public (anonymous) data

For data published in scientific journals, the underlying data will be made available no later than by journal publication. The data will be linked to the publication. Data associated with public deliverables will be shared once the deliverable has been approved and accepted by the EC. For other public datasets not directly linked to a scientific publication or deliverable, such datasets will be made available upon assessment by the responsible partner that it is ready for publishing, and in the final month of the project at the latest.

Open data can be reused in accordance with the Creative Commons licences. Data classified as confidential will as default is not reusable due to privacy/security concerns.

The public data will remain reusable via Zenodo for at least 20 years. This is currently the lifetime stated by the host laboratory CERN. If Zenodo has to close their operations, they have provided a guarantee that they will migrate all content (including metadata) to other suitable repositories.

Confidential (non-anonymous) data

All non-anonymous data will be deleted at the end of the project.

In case permission is given by the party providing and owning the data, some non-anonymous data will be kept for a maximum of 4 months after the contractual end date of the project[5]. The additional 4 months is to keep the underlying datasets available to allow the completion of any scientific publications being prepared towards the end of the project.

An exemption is pictures and videos, taken with consent from voluntary project/pilot/workshop/exercise participants, that are used for communication purposes. A consent form should be signed by any participant and a method should be provided to withdraw consent (e.g. sending an email). If consent is *not* withdrawn at an earlier time, such data will be kept for up to 4 years after the end of the project to comply with the EC contractual obligation to continue dissemination, communication and exploitation activities after the project ends. If a party withdraws the consent to use this material (pictures, videos), it will be deleted without delay.

4. Allocation of resources

Costs

SOTERIA uses standard tools and a free of charge research data repository. The costs of data management activities are limited to project management costs and will be covered by allocated resources in the project budget.

Long-term preservation of the public data is ensured through Zenodo. Other resources needed to support reuse of data after the project ends will be solved on a case-by-case basis.

Data Manager

BC3 as coordinator of the SOTERIA project is responsible for the data management. SINTEF provides support and has the responsibility of updating the Data Management Plan.

5. Data Security

In this chapter, the security features of the research data infrastructure used to store and handle data in the SOTERIA project are described.

Active Project - Data security as specified for BC3 Google Drive

BC3 Google Drive is the online collaboration platform used the SOTERIA project. A dedicated project

[5] At present, the contractual end date of the project is: 2026-02-28. However, changes can be made to this date during the project (e.g. in case of a project extension) and the final version of the DMP will provide the exact date.

site has been established on this platform, accessible only by the partner representatives in the consortium. Furthermore, a dedicated folder for research datasets will be set up, allowing for stricter access control than the main project site.

The SOTERIA GoogleDrive site has the following security settings:

- Access level: Restricted to persons (project members only). Further access restrictions on specific folders is enabled.
- Threat management, security monitoring, and file-/data integrity prevents and/or registers possible manipulation of data.

Documents and elements in the BC3 Google Drive sites are stored in Google's cloud solutions. There will be no use of data centres in the US or outside EU/EEA and associated countries[6].

Repository - Data security as specified for Zenodo

The following list describes the security settings for Zenodo:

- Versions: Data files are versioned. Records are not versioned. The uploaded data is archived as a Submission Information Package. Derivatives of data files are generated, but original content is never modified. Records can be retracted from public view; however, the data files and records are preserved.
- Replicas: All data files are stored in the CERN Data Centres, primarily Geneva, with replicas in Budapest. Data files are kept in multiple replicas in a distributed file system, which is backed up to tape on a nightly basis.
- Retention period: Items will be retained for the lifetime of the repository. The host laboratory of Zenodo CERN, has defined a lifetime for the repository of the next 20 years minimum.
- Functional preservation: Zenodo makes no promises of usability and understandability of deposited objects over time.
- File preservation: Data files and metadata are backed up nightly and replicated into multiple copies in the online system.
- Fixity and authenticity: All data files are stored along with an MD5 checksum of the file content.
- Files are regularly checked against their checksums to assure that file content remains constant.
- Succession plans: In case of closure of the repository, a guarantee has been made from Zenodo to migrate all content to suitable alternative institutional and/or subject based repositories.

6. Ethical Aspects

The proposed work in SOTERIA will fully comply with the regulations set out in Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR)[7]. In addition, SOTERIA comply with the

[6] EEA = Norway, Iceland, Liechtenstein

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of

principles of the European Charter for Researchers, the European Code of Conduct for Research Integrity, including ethical standards and guidelines, regardless country in which research is carried out.

Nothing in this project shall be deemed to require a party to breach any mandatory statutory law under which the party is operating. This includes any national or European regulations, rules and norms regarding ethics in conducting research.

Pictures and videos for communication purposes

SOTERIA will collect pictures and videos for use in communication activities (website, newsletter, social media). Such data will only be collected with prior consent from the people involved and only used for as long as consent is given. Pictures and video can contain personal data if an individual is the focus of the image or video. Examples include: 1) pictures/video of individuals stored together with personal details (e.g. identity cards); 2) pictures/video of individuals posted on the project website along with biographical details; 3) individual images published in a newsletter. Examples of pictures and video that is unlikely to contain personal data are: 1) pictures/video where people are incidentally included in an image or are not the focus (e.g. at a big conference/workshop); 2) images of people who are no longer alive (the GDPR only applies to living people).

When collecting pictures and video SOTERIA will follow established guidance and best practice on collecting and processing such data to ensure that we adhere to the legal requirements (e.g. guidance established by the University of Reading, UK[8]). Under no circumstances will pictures containing personal information be publicly shared without the subject's explicit consent.

7. Conclusions

Formal approval and release of this deliverable within the consortium constitutes a formal commitment by partners to adhere to the DMP and the procedures it defines. When the deliverable is formally approved by the European Commission, this constitutes confirmation that the procedures are considered by the European Commission to be adequate.

As coordinator of the SOTERIA project, BC3 will ensure that any data management issues which may arise during the project will be handled appropriately and in a transparent and fair manner.

The DMP is a living document that will expand as the project evolves and new information on data collection, generation and handling arise. Day to day data management will happen through the online tools described in this document, and through continuous collaboration between the partners responsible for data collection and generation in the project. A revised and extended version of this DMP will be prepared towards the end of the project to reflect the status of data management in the project.

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[8] https://www.reading.ac.uk/internal/imps/DataProtection/DataProtectionRequirements/imps-d-p-photographic.aspx

8. References

European Commission. H2020 Programme. Guidelines on FAIR Data Management in Horizon 2020. Version 3.0, 26 July 2016

European Commission. Horizon 2020 Programme. Guidelines to the Rules on Open Access to Scientific Publications and Open Access to Research Data in Horizon 2020. Version 3.2, 21 March 2017

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

ANNEX 1: Template for Data Processing Agreement

DATA PROCESSING AGREEMENT

Between

[ENTER DATA PROCESSOR], Company Reg. No. [xxx xxx xxx] ("**the Data Processor**")

and

[ENTER CLIENT/PARTNER], Company Reg. No. [xxx xxx xxx] ("**the Data Controller**")

being an agreement regarding the processing of personal data ("**the Agreement**") to be performed by the Data Processor on behalf of the Data Controller because of [ENTER BACKGROUND, e.g. agreement entered into with the Data Processor as the Supplier and the Data Controller as the Client dated [date] ("**the Principal Agreement**")].

1. The purpose of the agreement

The Data Processor shall process personal data on behalf of the Data Controller based on the background indicated above.

The purpose of the data processing, the duration and nature of the processing, the type of personal data to be processed and the categories of registered individuals are specified in attachments to this Agreement.

The Agreement shall ensure that personal data are processed in accordance with prevailing statutory requirements for processing personal data, including EU Directive 95/46/EF of 24 October 1995 on the protection of individuals relating to the processing of personal data and on the free movement of such data, which has been implemented in Norway through Act No. 31 of 14 April 2000 relating to the processing of personal data (the Personal Data Act) and associated statutory regulations, as well as the requirements pursuant to decree of the European Parliament and Council relating to the protection of individuals with regard to the processing of personal data and on the free movement of such data, superseding on 27 April 2016 Directive 95/46/EF (the Data Protection Directive), and Norwegian law and associated statutory regulations adopted pursuant to the Data Protection Directive and replacing the Norwegian Personal Data Act. Both the current and the subsequent Personal Data Act are referred to below as "the Personal Data Act".

The Data Processor shall process the personal data as described in the Agreement, and in other ways as may be agreed in writing between the Data Processor and the Data Controller.

Terms and definitions used in the Agreement shall be construed in the same way as in the Personal Data Act.

2. The rights and obligations of the Data Controller. The obligations of the Data Processor

The Data Controller shall ensure that the relevant personal data can be processed. Specifically, Data Controllers shall ensure that adequate legal authority exists and that the agreements entered into with the registered individuals and any consents given are commensurate with and facilitate the processing of personal data as specified in Attachment 1.

The Data Processor confirms that it will implement suitable technical and organisational measures to ensure that all processing pursuant to this Agreement satisfies the requirements of the Personal Data Act with respect to the protection of the rights of the registered individual, as well as complying with all the requirements of Article 32 of the Data Protection Directive. See also Section 4 for additional obligations. The Data Controller shall at all times maintain full legal ownership of the personal data.

The Data Processor shall only process personal data based on written instructions received from the Data Controller. The Data Processor shall always be able to provide documentation of such instructions. The Data Processor shall not process personal data to which it obtains access in any other manner than is necessary to carry out the assignments it receives from the Data Controller.

The Data Processor shall assist the Data Controller in responding to requests submitted by a registered individual wishing to exercise his or her rights pursuant to Chapter III of the Data Protection Directive, considering the nature of the processing, also assisting as far as possible by way of suitable technical and organisational measures. The Data Processor shall also assist the Data Controller by ensuring compliance with the requirements connected with personal data security and the assessment of the consequences for personal protection and prior consultation in Articles 32 to 36, taking into account the nature of the processing and the information available to the Data Processor. If approved standards of conduct exist, pursuant to Article 40 of the Data Protection Directive or approved certification pursuant to Article 42, with which the Data Processor has undertaken to comply or according to which it has undertaken to be certified, the Data Processor is obliged to comply with said standards of conduct or certification requirements.

The Data Processor shall maintain a log of processing activities it carries out on behalf of the Data Controller, which shall include at least the information specified by Article 30 of the Data Protection Directive. The Data Controller may at any time demand to be provided with a copy of such log.

The Data Processor shall make available to the Data Controller any information necessary to demonstrate that the obligations specified in this Section 2 are fulfilled, as well as facilitating and contributing to audits, including inspections, performed by the Data Controller or any other inspector authorised by the Data Controller. This also applies to providing access to security documentation. The Data Controller itself has direct responsibility for liaison with the relevant supervisory authorities.

The Data Processor has an obligation of secrecy with regard to personal data to which it obtains access as a consequence of the Agreement and its processing of personal data and shall ensure that persons authorised to process the personal data have undertaken to do so confidentially or are subject to appropriate statutory professional confidentiality. This provision applies also after the expiry of the Agreement.

The Data Processor shall not divulge data or information that it processes on behalf of the Data Controller to third parties without explicit instructions from the Data Controller. The Data Processor shall forward any enquiries received in this respect to the Data Controller without undue delay.

If the Data Processor is of the opinion that an instruction from the Data Controller conflicts with the Data Protection Directive, the Personal Data Act or any other regulation regarding the processing of personal data, the Data Processor shall immediately inform the Data Controller of this. The Data Processor undertakes to discharge its obligations pursuant to the Agreement irrespective of its opinion.

3. The use of sub-vendors

When processing personal data, the Data Processor shall only use sub-vendors (data processing sub-vendors) which have been approved in writing by the Data Controller and which have been confirmed as implementing suitable technical and organisational measures to ensure that processing pursuant to this Agreement complies with the requirements of the Personal Data Act and the need to protect the rights of registered individuals.

Approved data processing sub-vendors at the time of entry into the Agreement are specified in an attachment to the Agreement.

The Data Controller grants the Data Processor general permission to use data processing sub-vendors to process personal data pursuant to the Agreement. If the Data Processor plans to use other data processing sub-vendors or substitute other data processing sub-vendors, the Data Processor shall inform the Data Controller of such plans and give the Data Controller an opportunity to oppose such changes.

Any data processing sub-vendor shall be made familiar with the obligations of the Data Processor pursuant to this Agreement and with the regulations governing the processing of the Data Controller's personal data and shall be subject to the same obligations regarding the protection of personal data as are stipulated in the Agreement. The data processing sub-vendor shall furnish adequate guarantees that technical and organisational measures will be adopted to ensure that its processing complies with statutory requirements. If a data processing sub-vendor fails to satisfy its obligations regarding the protection of personal data and the requirements of the Agreement, the Data Processor shall assume full responsibility vis-à-vis the Data Controller for the sub-vendor's failure to satisfy those obligations.

4. Security and non-conformances

The Data Processor shall satisfy the requirements regarding security measures as specified by the Personal Data Act and associated statutory regulations. The Data Processor shall be able to document its procedures and other initiatives for satisfying these requirements. The documentation shall be made available to the Data Controller on request.

Security audits shall be carried out regularly at times agreed by the parties to the Agreement. An audit may embrace a review of procedures, random inspections, more comprehensive local inspections, and other appropriate verification measures. Agreement shall be reached regarding the Data Controller's obligation to cover the cost of any use of personnel and resources necessary in connection with the performance of such audits.

In the event of breach of security or personal protection stipulations, the Data Processor shall notify the Data Controller without undue delay. Such notification shall include at least the following:

1. A description of the nature of the breach of personal data security, including, wherever possible, the categories and approximate number of registered individuals affected, and the categories and approximate number of personal data records affected,

2. the name and contact details of the personal protection advisor or any other contact site at which additional information may be obtained,

3. a description of the probable consequences of the breach of personal data security,

4. a description of the measures taken or proposed to handle the breach, including where relevant measures for reducing any adverse effects resulting from the breach.

If all the information cannot be provided in the first instance, it shall be provided successively as soon as it becomes available.

The Data Controller is responsible for submitting notification to the supervisory authority and the Data Processor shall not submit such notification nor contact the supervisory authority unless instructed to do so by the Data Controller.

5. Transfer of data to foreign countries

Personal data shall only be transmitted to third countries outside the EU or EEA according to instructions from the Data Controller. The Data Processor shall therefore not transmit or allow parties in third countries in any way to obtain access to, personal data without explicit prior approval and instructions to this effect from the Data Controller. Consent and instructions must specify the countries to which the information may be transmitted. Even with consent and instructions, transfer to third countries shall only take place on condition that the requirements regarding security and the protection of the rights of the registered individuals pursuant to the Personal Data Act and other rules are satisfied.

6. The duration of the Agreement, termination orders, obligations in the event of expiry or cancellation

The Agreement is valid if the Data Processor processes or has access to personal data on behalf of the Data Controller pursuant to the Principal Agreement.

In the event of breach of this Agreement, the Personal Data Act or other relevant rules, the Data Controller is entitled to order the Data Processor to cease processing of the information with immediate effect.

On completion of the services connected with processing, the Data Processor shall, as instructed by the Data Controller, delete, or return any personal data to the Data Controller and delete all existing copies unless required by law to continue to store the personal data. This also applies to any back-up copies, where it is enough to overwrite according to established routines for back-up creation.

The Data Controller shall receive written confirmation from the Data Processor that all personal data have been returned or deleted according to the instructions of the Data Controller, and that the Data Processor has not retained copies, printouts, or personal data in any other form.

7. Other obligations and rights

Other obligations and rights ensue from the Principal Agreement between the Data Processor and the Data Controller regarding the services that necessitate the processing of personal data, and from this Agreement. The same contact representatives will serve in connection with this Agreement as for the Principal Agreement.

This Agreement shall not expand the Data Controller’s right to impose sanctions, including the Data Processor’s liability for damages, beyond the rights pursuant to the Principal Agreement.

In the event of conveyance of the Principal Agreement to other parties, this Agreement shall be conveyed correspondingly.

_____. _____ 2024

The Data Processor	**The Data Controller**
_____	_____
NAME	NAME

Two original copies of this Agreement have been prepared, of which each party has received one.

Attachments

The purpose of processing

[The purpose and intention of the processing shall be entered here.]

The duration of the processing

[Enter the length of time the processing shall take. If the processing is according to an agreement between the parties, the duration shall be expressed as "The processing shall last for as long as the Data Processor provides services to the Data Controller pursuant to the Principal Agreement.]

The nature of the processing

[Specify here what the processing consists of, for example, "Storage of personal data" or whatever circumstances necessitate the processing pursuant to the Principal Agreement.]

Types of personal data to be processed

The following types of personal data shall be processed pursuant to the Agreement:

[Enter the type of personal data, e.g. personal name, e-mail address, telephone number, etc. It is not necessary to give details of the information to be processed, only *the type* of information.]

Categories of registered individuals

[Specify categories of registered individuals, such as employees, clients, etc.]

Data processing sub-vendors at the time of entry into the Agreement

[Specify data processing sub-vendors and countries in which the data will be processed]

End Page