D7.3

Data Management Plan (DMP)

Date
28.03.2024

Authors: Nazli Aydin, Arka Bhattacharyya, Ali Cheshomi, Tina Comes, Nicolas Dintzner
Organisation: TU Delft

Funded by the European Union

Project funded by the European Union's Horizon Europe and the UK Research and Innovation (UKRI) programme under the UK government's Horizon Europe funding guarantee grant agreement n°10062626

Contents

D7.3 Data Management Plan

Revision v.3.0

Grant Agreement	101121356
UKRI numbers	10062626
Call identifier	HORIZON-CL3-2022-DRS-01
Project full name	AGnostic risk management for high Impact Low probability Events
Due Date	31.03.2024
Submission date	28.03.2024
Project start and end	01.10.2023 - 30.09.2027
Authors	Ali Cheshomi, Arka Bhattacharyya, Nazli Aydin, Tina Comes, Nicolas Dintzner

Abstract

The AGILE project's Data Management Plan (DMP) outlines how data is handled, covering organization, storage, sharing, and preservation, along with addressing ethical and legal concerns such as data security and protection. It provides guidelines for consortium members to safely manage personal data in line with regulations like GDPR and implements FAIR principles for datasets. All members must adhere to good data management practices and laws, ensuring transparency and reusability of research materials. The DMP is a dynamic document, comprising an overall project DMP and specific ones for each work package, completed on TU Delft's DMPonline platform for ongoing updates and monitoring.

Document revision history

Issue	Date	Comment	Author
V1.0	01.03.2024	First Draft	Ali Cheshomi, Arka Bhattacharyya
V2.0	13.03.2024	Updates & Revisions	Tina Comes, Nicolas Dintzner
V3.0	28.03.2024	Final version	Ali Cheshomi, Arka Bhattacharyya, Tina Comes

Acknowledgment

Project co-funded by the European Union's Horizon Europe and the UK Research and Innovation (UKRI) programme under the grant agreement n°10062626

Nature of the deliverable[1] **R**

Dissemination level

PU	Public, fully open. e.g., website	✔
SEN	Sensitive, limited under the conditions of the Grant Agreement	
CL	Classified information under the Commission Decision No2015/444	

[1] Deliverable types:
R: document, report (excluding periodic and final reports).
DEM: demonstrator, pilot, prototype, plan designs.
DEC: websites, patent filings, press and media actions, videos, etc.
OTHER: software, technical diagrams, etc.

Copyright notice

List of Tables

Abbreviations

DMP	Data Management Plan
WP	Work Package
HILP	High Impact Low Probability
GDPR	General Data Protection Regulation
UCL	University College London
TUD	Technische Universiteit Delft
FS	Factor Social
JUH	Johanniter-Unfall-Hilfe e.V.
PPI	Prepared International UG

Executive Summary

This Data Management Plan (DMP) describes how the AGILE project handles data. It details the organization, description, storage, sharing, and preservation of the research data collected, generated, and used in this research project, it also specifies ethical and legal matters concerning data security, data protection, and IPR issues. The DMP has set out guidelines for the consortium on how to handle personal data safely and securely in accordance with the national and EU ethical and legal requirements including the General Data Protection Regulation (GDPR) and developed provisional guidelines on how to implement the FAIR principles to the datasets.

All consortium members are responsible for complying with good data management practices and guidelines on the management and sharing of research data, data security and data protection in accordance with relevant legislations and research integrity. At the same time, researchers shall ensure the transparency and reusability of research materials produced and used in this project and see to that the degree of data openness and sharing is ethically and legally justifiable.

This DMP is a living document, including the overall project DMP as well as specific DMPs for each work package. Each DMP is follows the Horizon Europe template provided by the EU and is completed on the TU Delft's online platform DMPonline. These virtual DMPs will be updated, enriched, and facilitate monitoring as the project evolves.

Introduction

AGILE aims to develop a comprehensive framework and tools for managing High Impact Low Probability (HILP) events, drawing on various methodologies such as systems theory, strategic foresight, and machine learning. The project involves collaboration among research organizations, NGOs, SMEs, and authorities to create scalable methods for identifying vulnerabilities and recommending risk-informed system strengthening measures. Ultimately, AGILE seeks to enhance the strategic and operational risk management capacities of disaster stakeholders, contributing to societal resilience at local, regional, and national levels. The project's methodologies will enable better understanding, anticipation, and management of HILP events, supporting both proactive and reactive approaches to resilience-building. Its impact extends to key European and international policy priorities, including disaster risk management policies and climate adaptation strategies.

This document presents D7.3: AGILES's initial version of the data management plan (DMP), which describes the life cycle of data management for all datasets that are collected, generated, and processed by the research project. DMPs are essential documents that outline how research data will be managed, shared, and preserved throughout the research process. They ensure transparency, accountability, and compliance with funding agency requirements, addressing ethical and legal considerations while promoting data sharing and reproducibility. DMPs facilitate long-term access to research data, enhance risk management and data security, and improve research efficiency and impact by maximizing the usability and accessibility of data. Ultimately, DMPs play a crucial role in promoting responsible data stewardship, fostering research integrity, and advancing scientific progress by ensuring that research data are effectively managed, shared, and preserved for the benefit of society.

The guidelines defined in this DMP shall be followed by all members of the Consortium to ensure that research data are collected, transferred, analyzed, shared, or otherwise processed in a secure setting, that use of the data is in compliance with ethical and legal requirements, and that the openness, discoverability, and reusability of our research data are promoted as much as possible. If not noted otherwise, "data" refers to primary data collected purposefully for the AGILE project.

The aim for the DMP is to describe the datasets within the AGILE project, and to provide guidelines on data management to all partners in the project. This DMP as a living document will accompany the whole research life cycle, extending even after the active phase of the research project. If some specific guidelines requested at the time of this writing cannot be provided for, they will be updated as soon as the information about datasets becomes available.

Methodology

Our project's methodology for data management is designed to ensure compliance, efficiency, and security while fostering an environment of cooperation and transparency among all partners, following the EU's Horizon Europe template for data management. The process was supported by the TU Delft's faculty Technology, Policy & Management Data Steward who provided advise and feedback to the AGILE project members in the development of their DMPs.

This multifaceted approach follows the principles outlined hereunder:

Full Compliance with Legal Frameworks: At the forefront of our data management practices is the strict adherence to applicable EU and national laws on data protection. This includes the General Data Protection Regulation (GDPR) and Directive 95/46/EC, ensuring that all data processed within the project framework respects these regulations. Additionally, the project pledges to honor the data management policies of each participating organization, ensuring a respectful and compliant collaboration environment.

Development and Maintenance of a Public Data Management Plan: Central to our strategy is the formulation of a public DMP. This plan will articulate the methodologies for data processing under the GDPR definition, thereby providing a transparent framework for all project activities. The introduction of an AGILE DMP, alongside those developed by individual partners, aims to enhance research efficiency significantly. This approach not only ensures agility in our processes but also fortifies data security and minimizes risks associated with data handling.

Adherence to FAIR Principles: The management of all data and services generated by the project will align with the FAIR principles, embodying our commitment to making data Findable, Accessible, Interoperable, and Reusable. This commitment extends to working with federated data within the project and sharing data with external partners and communities, underscoring our dedication to collaborative and open research practices.

Uniform Structure and Coherence Across Work Packages: By leveraging the TU Delft Data Management Plan template, we have instituted a uniform structure for DMPs across all work packages. This uniformity ensures coherence and consistency, integral to the project's success. We have systematically guided work package leaders to align their plans with both the TU Delft template and EU protocols, fostering a unified data management approach.

Effective Communication, Collaboration and Transparency: The methodology's effectiveness is further augmented by engaging task leads in promoting efficient communication and adherence to data management standards. A collaborative effort with the faculty data steward has been instrumental in the review and refinement of all DMPs, ensuring each plan meets the project's stringent requirements. In addition, this approach allowed us to identify interdependencies between WPs, and we will be working on the required steps (data sharing agreements) over the next weeks.

Central Repository for Easy Access: To facilitate ease of access and oversight, we make use of the TU Delft's DMPonline tool (https://dmponline.tudelft.nl, see Table 1). This table providing links to each work package's DMP, serves as a centralized access point

for all project members, making detailed information on data management practices readily accessible, and facilitating continuous monitoring, oversight and risk management.

Through these dimensions, our methodology not only addresses the immediate needs of the project but also lays the groundwork for long-term success and compliance. By embracing a holistic approach to data management, we aim to achieve our objectives efficiently, securely, and in full alignment with established legal and ethical standards.

Results and Implementation

Our comprehensive DMP integrates the overarching principles of data management for the project with specific plans from each work package, outlining uniform practices for data collection, storage, sharing, and security. A central repository has been established via the TU Delft's DMPonline tool, following the standards put forward by the EU under the Horizon Europe template.

Table 1 provides immediate access to individual 'living document' DMPs via a master table. These will be maintained throughout the project's lifetime. This table not only simplifies navigation but also ensures transparency and facilitates continuous monitoring and compliance checks. Each DMP is also provided as an Annex as indicated in Table 1.

Table 1. Link to AGILE's Data Management Plan

WP	WP Title	Lead	Link to the DMP	Annex
	Overall project DMP	JUH	https://dmponline.tudelft.nl/plans/145440	A
1	Conceptualising HILP as concurrent, cascading and systemic events	UCL	https://dmponline.tudelft.nl/plans/146023	B
2	Multi-Disciplinary HILP Reference Library	TUD	https://dmponline.tudelft.nl/plans/144150	C
3	Risk and resilience stress-test methodology	FS	https://dmponline.tudelft.nl/plans/147020	D
4	Scenario co-development and stress test implementation	JUH	https://dmponline.tudelft.nl/plans/144499	E
5	Evidence-based planning, capacity building and risk communication	PPI	https://dmponline.tudelft.nl/plans/146704	F
6	High Impact Creation - Dissemination, communication and exploitation	ARTTIC	https://dmponline.tudelft.nl/plans/144167	G
7-8	Project coordination and management / Ethics requirements	JUH	https://dmponline.tudelft.nl/plans/144146	H

Conclusions

The AGILE project's DMP is subject to ongoing monitoring and updates, managed by the project management team, to ensure it remains congruent with the latest project developments and European Union guidelines. This iterative process is vital for maintaining the DMP's relevance and efficacy, allowing for the incorporation of new insights and adjustments in data management practices as the project progresses. The next versions are scheduled for submission in Month 18, 36, 48 incorporating insights and advancements from the ongoing project.

Appendix

Annex A:

Plan Overview

A Data Management Plan created using DMPonline

Title: Agile Consortium - Project level Data Management Plan

Creator: Nicolas Dintzner

Affiliation: Delft University of Technology

Funder: European Commission

Template: Horizon Europe Template

ID: 145440

Last modified: 29-02-2024

Agile Consortium - Project level Data Management Plan

Data Summary

Will you re-use any existing data and what will you re-use it for?

To the extent it is possible, project members will rely on already available dataset as to ease the creation of new knowledge in the context of the AGILE Project.
Such datasets will be:
already publicly available, in which case, project members will be in charge of ensuring proper reuse of the data (e.g. licensing concerns)
made available upon request by project partners or other institutions, in which case, the acquisition of this data must follow institutional rules (data sharing agreement)

What types and formats of data will the project generate or re-use?

Project members are expected to generate various data across a range of WPs as indicated in the individual DMPs per WP. The project aims to maximise re-use. To facilitate re-usability of the produced and re-used data, the consortium commits to the use of file formats that are "Open". Preferred format will text based (.rtf/.txt, .csv, any source code format).

Commonly used formats such as .docx and .xlsx (Office format) are also reasonable (the format is openly documented and such files can be opened and processed using LibreOffice for instance).
Specific file formats may lead to additional constrains during the project as those may require specific tools. Provision of such tools for all relevant partners (if needed) can be planned for.
At the project level, the Coordinator will ensure that the following information is readily available:

- meeting minutes
- project progress reports
- data management plans per WP
- risk management documents and monitoring
- Submitted, planned and ongoing deliverables
- General documentation of the project (proposal, consortium agreements, approval letters from funder, time planning, stakeholder list, ... which could be of use to all partners during the execution of the project)

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

All data generated during the project will support one or more expected deliverable of the project.
The data can be created (or prepared):

- for communication purposes with partners (e.g. subset of confidential information)
- research and innovation activities (WPs and tasks)
- communication and outreach purposes

Any use of the data that is not planned in the project is feasible, provided partners refer to the Coordinator and ensure that this does not negatively impact other project members.

What is the expected size of the data that you intend to generate or re-use?

Each institution is in charge of the storage of the data and material they need. They must ensure to have adequate storage (including need-basis access rights, automated backup procedure, perhaps institutional approval for the usage of said storage for the data they have). Partners may experience storage issue if the volume of data generated or shared is large. Partners should plan ahead how much storage space they expect to need for the overall duration of the project.
For the project level data made available to all project members, we will rely on SharePoint which offers sufficient storage space for the purpose of project administration.

What is the origin/provenance of the data, either generated or re-used?

Each partner is in charge of tracking data provenance. This is particularly important for:

- reuse of already available material, as to ease license and IP related verification

- data issued by partner organization, as to ensure that proper credit is given, and that the mean of transfer (data agreement) are in place.

Specific attention should be given to data sharing requiring specific agreements to be put in place. **Should a partner institution know that they want to get access to sensitive information from other partners, this should be clearly stated here.Likewise, if a partner organization knows that they will make some data available to other, this should be stated here.** The issuer of the data will be in charge of communicating the requirements that need to be fulfilled for the adequate transfer of the data.

To whom might your data be useful ('data utility'), outside your project?

The data produced by each work-package will fulfil part of the expected impact of the project. A short description of the targeted audience can be provided in each WP DMP.
The data produced at a project level is aimed at facilitating the execution of the project and communicating the results, and is only meant to be used by the research consortium itself, and reporting to the funder.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

To the extent it is possible, all partners will make sure that the data produced in the project can be made safely publicly available (non-personal, non-confidential).
All public datasets should be uploaded in a research data repository (e.g. Zenodo, or 4TU Research Data). The choice of repository is left to each partner, depending on which repository is most suitable for the data they produce and the domain they address. However, the following section will outline what is considered as suitable characteristics of the chosen repository - for publicly available material (non-confidential, non-personal)
The chosen data repository must provide a persistent identifier to each uploaded dataset (DOI, or Handle).

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

The chosen data repository must provide metadata for each dataset which is compliant with standards such as DublinCore or DataCite, as to ensure discoverability of the datasets.
Each partner should rely on existing meta-data standard for the formatting of the data itself. If no such standard exist (which is currently quite likely), documentation regarding the "shape" of the data (units, boundary values, semantic) must be provided in the form of text (README file)

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

All research data repository provide keywords - partners are to ensure that this is the case for the repository where the publicly available data is archived.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

Most research data repositories allow metadata of dataset to be harvested and indexed, by making this information available under a specific CC-0 license (the dataset itself is distributed under a license chosen by the uploader of the data). Zenodo and 4TU Research data repository do provide such features.
If partners rely on another research data repository, they should asses whether such features are available in the chosen repository.

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

Repository which have the "CoreTrustSeal" certification will be considered trusted. Zenodo or 4TU Research Data have this certification.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

Most research data repositories are publicly accessible and allow for a maximum amount of data to be stored per user (and potentially per year). It is up to each project partner to estimate if the storage space made available to them by their repository of choice is suitable.
Maximal volume of data for Zenodo is: 50GB per dataset, but users may upload any number of datasets.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

The chosen data repository must provide a persistent identifier to each uploaded dataset (DOI, or Handle).

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating

legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

Only data that can be made publicly available (non-personal, non-confidential) will be uploaded into any research data repository.
All datasets uploaded in such repository must be given an open license (CC-like for data, Apache-like for software). Each partner institution is in charge of checking that they are allowed to apply license of uploaded material.
Data which cannot be made openly available will be preserved by relevant partners at least for the duration of the project. Data access protocols will be part of the supplementary material of publication (if the data cannot be made available, to process to acquire it can be shared e.g.: *data is held by [institution X] and access to the data requires [appropriate data agreement]*).

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Embargo, or limitation to data publishing must be discussed among all project partners as to ensure that the publication does not cause undue damages.
Discussion regarding embargo should be taking place at a project level when it deals with data shared between partner institutions. Such expectation, mostly valuable in the case of sensitive or confidential data sharing between partners must be set out in the appropriate data sharing agreement if such agreement are needed.

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

Standardized and free access protocols to openly accessible data are ensured by trusted repositories.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

During the project, each partner is in charge of granting access (under condition set by them) to relevant partners, on a need-basis - as data subject to restrictions will be confidential or personal in nature. Each issuer of data is in charge of providing access during the project.
Access to non-public data after the project will depend on each institution policy, but general expectation regarding long-term (post-project) data availability should be mentioned in the WP Data Management Plan.

Legal constrains, such as GDPR or AI Act, may force deletion of part (or all) of the collected material at a specific point in time.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

Checking identity of people accessible data is relevant when:

- confidential data is to be shared / made accessible to specific member of a WP (partners). Each institution sharing material is in charge of ensure that only the targeted member(s) of partner institution will be granted access (need-basis)

Should the use of restricted access archive (as offered by Zenodo or 4TU) is used by a partner, the partner institution that used this feature will have to ensure that they have the means to check the appropriateness of access requests.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

During the project, questions related to data sharing or access by partners to data sources (either from other partners or other external sources) can be discussed within the project team. For the time being, the PI is the first point of contact for such concerns.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

Such features are provided by research data repositories.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

Such features are provided by research data repositories.

2.2. Making data accessible - Metadata:

Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

Research material that can be made publicly available should be documented, including the information about the tools that are needed to work with the data if needed.
If possible, software prototypes and demonstrators (source code) produced in the project should be made publicly available - unless publication exposes partners to confidentiality problems.

2.3. Making data interoperable:

What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

Partner are in charge of following standard vocabularies available in their fields if such exists (HDX provide some of it which may be of use).
In most cases, such vocabularies / standards will not be readily available, and the interoperability of the data will be supported by documentation in an open format (README files in text). The content of each readme file will follow best practices in the domain.

2.3. Making data interoperable:

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

In most cases, such vocabularies / standards will not be readily available, and the interoperability of the data will be supported by documentation in an open format (README files in text). The content of each readme file will follow best practices in the domain.
Many guidelines are available regarding how to format README file. One example of such documentation is presented here :
https://data.4tu.nl/s/documents/Guidelines_for_creating_a_README_file.pdf

2.3. Making data interoperable:

Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

Should published dataset be derived from one or more other existing datasets, this information will be provided along side of the published dataset. This can be done through

the metadata standard offered by the research data repository, or will documented in the associated README file.

2.4. Increase data re-use:
How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

The published material (non-personal/non-confidential) will contain all relevant data and software prototypes and demonstrators, with the appropriate documentation.

2.4. Increase data re-use:
Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

Each institution is in charge of ensuring that they can apply open licenses to material that is made publicly accessible.
It is expected that public data is made available under a CC-like license, and software under a Apache-like license.

2.4. Increase data re-use:
Will the data produced in the project be useable by third parties, in particular after the end of the project?

Publicly available data is expected to be reused by anyone, any where in the world.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

Provenance of the data must be documented as part of the scientific publication - most research data repository offer a "Cite me" button which will help to follow standards (citation format).

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

All datasets which can be made publicly available will be recorded by the PI. The record will contain the name of the dataset, the issuer/owner/research team that produced it, a link to the data, and the license that is used.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

Each partner institution is charge of ensure that their storage solutions provides adequate security for the data they produce (personal, confidential data), with sufficient storage space.
Each partner institution is also in charge of ensure that they follow their appropriate ethical protocols (IRB review or others). Letters of approval from such review process can be included as part of the research output (for safe keeping and reference).

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

As indicated in the DoA, in the AGILE project we expect all deliverables to be in digital format (reports or software deliverables), or digitalizable (written notes).

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

Each WP leader is responsible for providing data management plans for their specific work package.
The DMPs will be linked to this Project-Level DMP (in the description), overseen by the project coordinator. Those initial DMPs may be enhanced by smaller, more targeted DMPs for specific protocols - as per research institution regulations or other requirements.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.)?

Each WP can estimate the cost of data management. This should already be accounted for in the budget of the project. If not, WP leader can get in touch with the project coordinator as to determine what can be included or not based on the approved budget.
Research output may include additional outputs such as the prototype of a service or online platform. The cost associated with the management of said platform (including the hosting, operation, and legal consideration) should be considered - at least for the duration of the project, and plan for long term support should be considered as well.

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

See above.

Who will be responsible for data management in your project?

The data management is overseen by the Coordinator of the project, who will mandate a specific partner as a main reference point for data related questions.

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

4TU Research Data and Zenodo offer relatively cheap storage solution for long term archival of publicly available data.
In the case of very large datasets which cannot be archived as-is, the WP leader will be in charge (in cooperation with the appropriate task leader) to determine if a smaller version (toy example, subset, ...) could be of use while still fulfilling the objective of ease of reuse and validation of the core results.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

Each WP leader is in charge of ensure that the storage solution provided by their institution is sufficiently secure to store the data that they create or obtain from partners.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

We expect that confidential and personal data will be processed during this project.
Each partner is in charge of ensure that confidential and personal data transfer between institution is done in a lawful manner (GDPR- compliance, including data sharing / processing agreements) are in place.

Personal or confidential data sharing are do inherently expose institution and people to additional risks which should be taken into account during ethical review.
Establishing such agreement is time-consuming and partner institutions are invited to outline here what data exchange they expect to participate in, such that the agreements can be established as early as possible.

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

Informed consent - when used - will outline what data is collected, where it is stored, and what is made public and what is deleted (if relevant).

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

Each institution can indicate here specific protocol that they intend to follow if such document exists and can be shared publicly.
It will be expected that each institution follows their institutional regulation.

Annex B:

Plan Overview

A Data Management Plan created using DMPonline

Title: Agile Consortium - WP1

Creator: Lauren McMillan

Principal Investigator: Gianluca Pescaroli

Data Manager: Gianluca Pescaroli

Contributor: Mhari Gordon, Lauren McMillan

Affiliation: University College London

Funder: European Commission

Template: Horizon Europe Template

ORCID iD: 0000-0003-3468-2970

Project abstract:

The AGILE project aims to design, develop, and apply a holistic methodological framework and practical tools for understanding, anticipating, and managing HILP events with a systematic risk and resilience perspective. To better understand deal and live with High Impact Low Probability (HILPs) events, it is important that policy makers and risk assessors are equipped with appropriate understanding of how to address capacity to multiple system failures. The AGILE project offers novel research on HILPs understanding as it is co-created with a transdisciplinary consortium of research organisations, non-governmental organisations (NGOs), small and medium enterprises (SMEs), as well as local and regional authorities.

Work package (WP) 1 will establish the scientific backbone of the AGILE project regarding HILP risk management. This WP conceptualises HILPs as concurrent, cascading and systemic events and develops a taxonomy for HILP events. WP1 aims to identify common conditions between HILP and HIHP events, propose a consistent approach for assessing drivers of escalation and common point of failure, and define the possible use of creative/lateral thinking for systematising an approach to tabletop exercises and scenario building.

ID: 146023

Start date: 01-10-2023

End date: 01-10-2024

Last modified: 05-03-2024

Grant number / URL: https://cordis.europa.eu/project/id/101121356

Agile Consortium - WP1

Data Summary

Will you re-use any existing data and what will you re-use it for?

No existing data will be re-used.

What types and formats of data will the project generate or re-use?

WP1 will generate data through interviews and focus groups. Experts in risk and resilience will be invited to interviews and focus groups to discuss their opinions on the conceptualisation of HILPs and the challenges of planning for and managing HILP events. As part of this process, the UCL team will receive personal data on participants as well as the transcripts and notes from interviews and focus groups. This will be in the form of text data, and may include video or audio files if the participant consents. Whenever possible, we will use file formats suitable for long-term preservation and re-use of research data. Quantitative data will be stored in .csv format and qualitative interviews and metadata will be stored in .txt format. Audio and video data, if gathered, will be stored in .mp4 format or equivalent.

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

The personal data for participants is necessary for the administration of the interview/focus group process, and to ensure that appropriate experts are consulted for this task.
The data gathered from interviews/focus groups will be used to understand expert opinions on the underlying theory of HILPs, as well as to assess the current state of the operational landscape regarding HILP management. This will be used to develop the AGILE theory of HILPs and to inform the theory behind later development of stress testing methodology, to align with operational practices and concerns.

What is the expected size of the data that you intend to generate or re-use?

We expect to generate no more than 1TB of data. For data storage, space will be requested through the UCL Research Data Storage Service.

What is the origin/provenance of the data, either generated or re-used?

In order to select interview/focus group participants, some personal data (name, job title, company etc.) of potential participants will be gathered from other project partners, from existing connections of the UCL data, or found via LinkedIn.
Data for this WP will originate from the interview/focus group discussions.
The collection, storage, and anonymisation processes for this data are all addressed within a low-risk ethics application made to UCL for these interviews/focus groups.

To whom might your data be useful ('data utility'), outside your project?

The collected data will be useful for academics and researchers in the field of disaster resilience. It will also be useful for public policy making.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

Transcript data and personal information on participants will not be made available beyond the project team. Any publications that make use of the data will be assigned a Digital Object Identifier (DOI), to make them citable and persistently available. We will ensure that no confidential data that contains private information is published. We will also ensure that consent is obtained to share opinions from interviews/focus groups in publications (subject to anonymisation).

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP. Any publications as a result of this WP will create metadata per the journal/publisher's standard practice.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP. Any publications as a result of this WP will have relevant keywords.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.
Personal data of interview/focus group participants will not be made openly available due to privacy and security concerns.
The text (and potentially video and audio) data generated by interviews/focus groups will also not be made openly available. This is out of privacy and security concerns. However, selected quotes from participants may be included (after anonymisation) in publications resulting from this work, subject to the consent of the participant.

2.2. Making data accessible - Data:

If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Discussion regarding embargo will take place at a project level when it deals with data sharing between partner institutions. Any expectations, particularly in the case of sensitive or confidential data sharing between partners, must be set out in an appropriate data-sharing agreement if such agreements are needed.

2.2. Making data accessible - Data:

Will the data be accessible through a free and standardized access protocol?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Data:

If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

Personal data on the participants of interview/focus groups will not be shared beyond the UCL team, with the exception being when partners share the information of potential participants from their wider network. Video/audio data will not be shared beyond the UCL team to ensure the participants remain anonymous.
Anonymised text data from interviews and focus groups will be shared with the wider AGILE consortium (but not made available publicly). This will be done in accordance with secure data-sharing protocols. The data will be stored up until at least the end of the project.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

We will ensure the integrity of the data by providing a secure and safe environment through dedicated log-ins. To implement this, we will seek help from the institutional services at UCL.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

We do not foresee a need for a data access committee for this WP, given that the shared data will be fully anonymised and shared only within the AGILE consortium.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.
The data shared within the AGILE team will remain available until at least the end of the project.

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.
No software will be necessary to access or read the data shared within the AGILE consortium.

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.3. Making data interoperable:
In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.3. Making data interoperable:

Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.
For data shared within the AGILE consortium, we do not anticipate many qualified references. However, it is possible that participants in interviews/focus groups will refer to documents or sources during discussions, and in this case the UCL team will seek to find an appropriate reference and insert this into the text data (following completion of the interview/focus group).

2.4. Increase data re-use:

How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP. We do not anticipate a need for any additional documentation to validate data re-use for the data shared within the AGILE consortium.

2.4. Increase data re-use:

Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.4. Increase data re-use:

Will the data produced in the project be useable by third parties, in particular after the end of the project?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

As above, no datasets will be made publicly available beyond the AGILE team as a result of this WP.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

Data generated by interviews/focus groups will be subject to a screening by the UCL team to ensure that there are no errors in notes or transcripts that impact the clarity of the data.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

As addressed earlier, any data featured in publications as a result of this WP will be anonymised. Data will be gathered and stored securely, following data security standards. A low-risk ethics application has been made to UCL's Institute for Risk and Disaster Reduction for the planned interviews and focus groups.

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

We expect all outputs to be digital.

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

We will ensure that all publicly available research outputs are FAIR.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

The expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.

How will these be covered? Note 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 expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.

Who will be responsible for data management in your project?

Persons responsible for the data management for AGILE WP1 are Gianluca Pescaroli (lead), Lauren McMillan, and Mhari Gordon.

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

The UCL Research Data Repository will be used to securely store any data that must be archived and preserved beyond the end of the project. The AGILE consortium will agree upon what data will be kept and for how long - these discussions may occur at steering committee meetings or security council meetings as appropriate.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

We will use UCL's Research Data Storage Service, where data is fully backed-up daily. Specialist technical support is available to help with using this service.
Only UCL team members have access to the designated server, limited to the lead scientific advisor of the project (Dr Gianluca Pescaroli), Dr Lauren McMillan, Dr Sarah Dryhurst, Prof Maureen Fordham, Prof Mark Pelling, Dr Saman Ghaffarian, and Mhari Gordon. The storage security is ensured by UCL ICT services.
The UCL Research Data Repository will be used to securely store any data that must be archived and preserved beyond the end of the project.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

A low-risk ethics application has been made to UCL's Institute for Risk and Disaster Reduction for the planned interviews and focus groups. Ethics approval will be a deliverable for this WP.
All data will be anonymised before sharing beyond the UCL team.

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

All participants in interviews/focus groups will be asked for their consent to share their personal details with the UCL team, as well as their consent to share anonymised versions of any text data with the AGILE consortium. All data will be anonymised before sharing beyond the UCL team. This will be included in the pre-interview/focus group participant information sheet and participants will have the option to cease their involvement at any time during the interview/focus group. For the duration of the project, any participants can request that their data be removed for any reason. Long-term plans for preserving data will be presented to participants in the information sheet and subject to their approval.

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

Data management will comply with the UCL Research Data Policy. This policy ensures research data management aligns with the UK Data Protection Act (2018), European General Data Protection Regulation (2018).

Annex C:

Plan Overview

A Data Management Plan created using DMPonline
Title: AGILE_WP2
Creator: Arka Bhattacharyya
Affiliation: Delft University of Technology
Funder: European Commission
Template: Horizon Europe Template

Project abstract:

This work package essentially develops the computational backbone of this project. Here, we will utilize the advances in the information and data collection to establish an architecture and database of HILP events, which will be further used for Machine Learning based analysis of those events. Through a literature review and stakeholder engagement, a comprehensive classification and taxonomy of HILP events will be created leading to the identification of prominent variables that influence the outcomes of HILP events. The design and implementation of a reference library and database will integrate global open data such as HDX. Copernicus, NASA, Our World Data, etc., and Pacific Disaster Center's disaster event data, enhanced with infrastructure, social, economic, and governance indicators. Machine learning techniques such as unsupervised methods like Principal Component Analysis or Self Organizing Maps, will analyze patterns driving HILP events and inform the development of intervention guidelines and mitigation measures. The platform's interface will be user-friendly, allowing for rapid queries and comparative analysis of HILP events, while ensuring data integrity and security. Stakeholder feedback and validation will refine the platform's design and enhance its usability, ultimately contributing to the AGILE toolkit's accessibility and effectiveness in disaster response and management.
ID: 144150
Last modified: 26-03-2024
AGILE_WP2

Data Summary

Will you re-use any existing data and what will you re-use it for?

We plan to collect data from different project partners and open sources such as HDX, Copernicus, NASA, Our World in Data, etc. The collected data will be used to develop database of past High Impact Low Probability (HILP) events, which will subsequently be used to develop machine learning models to analyze HILP events.

What types and formats of data will the project generate or re-use?

We plan to conduct a survey of the stakeholders involved in this project. In the survey, a mix of qualitative and quantitative data will be collected. The objective for the data collection is to understand the requirements for the HILP reference library and database. For creating the reference library and HILP event database, we will also collect data from

open access data sources like HDX, Copernicus, NASA, Our World Data, etc. Whenever possible, we will use file formats suitable for long-term preservation and re-use of research data. Quantitative data will be stored in .csv format and qualitative interviews and metadata will be stored in .txt format.

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

There are two purposes. First, we will conduct a survey of the stakeholders to understand the requirements of the proposed HILP reference library and database. Second, we will collect data from open access data sources like HDX, Copernicus, NASA, Our World in Data, etc., to develop the proposed HILP reference library and database. The database will then be used to develop machine learning models for analyzing HILP events.

What is the expected size of the data that you intend to generate or re-use?

We expect the collected data to size between 250 GB and 5 TB. We will request TU Delft Self Service for the data storage.

What is the origin/provenance of the data, either generated or re-used?

Data for this WP will be collected from stakeholders' survey and open access data sources such as HDX, Copernicus, NASA, Our World in Data, etc. Specific attention will be given to the license under which the data is distributed. We will obtain data from PDC. The protocol to obtain data will be established before the transfer takes place.

To whom might your data be useful ('data utility'), outside your project?

The collected data will be useful for academics, researchers in the field of disaster resilience. It will also be useful for public policy making.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

All datasets will be assigned a Digital Object Identifier (DOI), to make them citable and persistently available. We will use appropriate data repositories like Zenodo or 4TU Research data for uploading and storing the data. We will ensure that no confidential data that contains private information is published.

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or

general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

All data will be made openly available through Zenodo or 4TU.ResearchData, a trusted and certified data repository. All datasets will be accompanied by rich metadata, adhering to the DataCite Metadata Standard, to ensure that they are findable.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

All data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU.ResearchData. To further aid their discoverability, keywords describing the datasets will be added.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

Both Zenodo and 4TU.Research Data make metadata available under cc0 license such that it can be harvested.

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

All data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU.ResearchData, both trusted and certified data repositories. Both repositories have CoreTrustSeal certification. All the data will have DOI for persistent identification and will be stored for at least 10 years.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

We will make specific arrangements to make sure the whole HILP reference library and database is archived. We will figure out this throughout the duration of the project. Both Zenodo and 4TU.ResearchData offers sufficient space to store the data.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

All data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU.ResearchData. Both repositories ensure DOIs for datasets.

2.2. **Making data accessible - Data:**
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

We plan to collect data from different project partners and open sources such as HDX, Copernicus, NASA, Our World in Data, etc. We will abide by the license of different databases. No confidential data containing private information will be made openly available. If the data is obtained from the project partners, we will consult them for license matters before publishing.

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

We do not expect any embargo period for the data that we plan to make openly available through trusted repositories.

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

Yes, this will be provided by the trusted repositories we have identified.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

We will not publish any confidential data containing private information. Therefore, we do not expect any restricted access to the published data.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

We will ensure the integrity of the database by providing a secure and safe environment through dedicated log-ins. To implement this, we will seek help from the institutional legal services at TU Delft.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

We do not foresee a need for anything like this for this work package.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

The trusted repositories will make the metadata openly available and licensed under a public domain dedication CC0, as per the grant agreement.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

We will preserve the data for at least 10 years for everyone. The trusted repositories guarantee the preservation of the metadata after the data is no longer available.

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

All datasets will have the necessary documentation containing the description of the tools to re-run the experiment ensuring reproducibility.

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

We plan to collect data from HDX database. HDX has metadata standards. We will abide by that standard for the all the datasets.

2.3. Making data interoperable:
In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

We plan to use the existing ontologies and vocabularies. If that is not possible, we will explain the generated ontologies and vocabularies to allow reusing, refining, or extending them. This will be part of the dataset documentation.

2.3. Making data interoperable:

Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

Yes, relevant references will be included in the metadata of the datasets.

2.4. Increase data re-use:

How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

All documentation needed to validate data analysis and facilitate data re-use will accompany the data via a README file created in accordance with the 4TU.ResearchData guidelines.

2.4. Increase data re-use:

Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

Yes, we will find open license for all the datasets. All material will have CC-like license ensuring free availability in the public domain and widest possible re-use, in line with the grant agreement.

2.4. Increase data re-use:

Will the data produced in the project be useable by third parties, in particular after the end of the project?

Yes, we will make all the data except for confidential ones containing private information available to all.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

Yes, see section 2.3.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

We will rely on the best practices on the domain and call on the data support team at TU Delft.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

We will conduct a survey, which will be reviewed by the TU Delft Ethics Committee. We will ensure that no personal data is made available without the consent of the respondent. We do not expect any data security concerns for this work package.

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

We expect all outputs to be digital as per section 1.

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

We will ensure that all publicly available research outputs are FAIR. All datasets will be granted a DOI, an open license and will be documented.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

The expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

These costs will be covered by the suggested budget.

Who will be responsible for data management in your project?

Persons responsible for the data management for AGILE WP2 are Tina Comes, Nazli Yonca Aydin, and Arka Bhattacharyya.

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

We will preserve the data to the extent possible through the trusted repositories. Any confidential data that cannot be made public will be preserved in private storage at least for the duration of the project.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

We will use TU Delft approved storage solution, where data is backed up automatically.
During the course of the research project, all data will be stored on local servers maintained and automatically backed up by TU Delft ICT. Every night the data will be automatically backed up. The data will be replicated over multiple sites/data centers. Data can be recovered with the help of TU Delft ICT services in the event of an incident.
Only team members have access to the designated server, limited to the principal investigator of the project (Prof. Tina Comes), Prof. Nazli Yonca Aydin, and Arka Bhattacharyya. The storage security is ensured by TU Delft ICT services.
The Faculty Data Steward will provide additional advice, as needed, on data storage during the research project. This data storage solution offers secure storage and transfer.

After the end of the project, all datasets will be published in Xenodo or 4TU.ResearchData. The data will be openly accessible to all.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

Any research protocol involving humans will be reviewed by TU Delft Ethics Committee. Letters of Approval from the Ethics Committee will be part of the project deliverables.

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

For the survey, we expect to collect personal data. Long term preservation strategy for the collected data will be presented to the participants and subject to their approvals.

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

We are going to be in compliance with the TU Delft Research Data Framework Policy stating that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so.

Annex D:

Plan Overview

A Data Management Plan created using DMPonline
Title: AGILE WP3
Creator: Beatriz Rosa
Affiliation: Other
Funder: European Commission
Template: Horizon Europe Template

Project abstract:

WP3 will collect and generate knowledge related to existing Stress Testing approaches, which will form the basis for the development of the integrated risk and resilience Stress Testing methodology and toolkit. This toolkit will build on the key concept of the tiered ST approach and will integrate novel approaches and methodologies.
ID: 147020
Last modified: 13-03-2024
AGILE WP3

Data Summary

Will you re-use any existing data and what will you re-use it for?

Whenever possible, we will use existing datasets to facilitate the generation of new knowledge within the AGILE Project framework. This includes publicly available and open-source data, for which project members will be responsible to comply with the appropriate reuse, addressing concerns such as licensing, and datasets that might be made accessible upon request from either project partners or other institutions, requiring adherence to institutional regulations for data acquisition, such as data sharing agreements.
The data will be used to gather knowledge related to stress testing, develop a framework which will be the basis for the development of an integrated risk and resilience stress testing methodology.

What types and formats of data will the project generate or re-use?

To ensure reusability and long-term preservation of research data, we plan to use commonly used formats that are open and text based (e.g., .cvs, .txt, .docx, .xlsx, .ipynb, etc.) as much as possible, as well as spatial/location-based data. We plan to use NetCDF for climatic data, .tif data for satellite images, .shp for vectorial data. The developments of the unfolding activities will lead to a greater definition of data related aspects, refining and tailoring the approach to Data management (e.g. more detailed information on input and output formats etc..).

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

The data used and generated during the project will support research and innovation activities within WP3 with the purpose of developing a framework and methodology for risk and resilience stress Testing. More specifically, the data will serve two objectives: (1) developing the stress testing methodological framework to map systems' interdependencies in economic, social, and physical domains; and (2) developing the methodologies for identifying and managing systems resilience to HILP events, including strength and direction of cascading failures, to enhance infrastructure preparedness and community resilience.

What is the expected size of the data that you intend to generate or re-use?

The size of the data will be defined at a later stage once the research environments are at a more advanced phase, and we are able to have a clearer idea of this information. Either way, each institution is in charge of the storage of the data and material they use and generate. Therefore, within WP3, task leaders must make sure they have adequate storage. We do not expect WP3 to require more than 1 TB of data.

What is the origin/provenance of the data, either generated or re-used?

Data will be collected from open data sources to the extent that it is possible. Any additional data obtained upon request will be supplied by project partners or other institutions. For both existing and requested or generated data, careful consideration will be given to licensing, proper credit attribution, and the implementation of data sharing agreements when necessary. Protocols for accessing sensitive information will be communicated and established if the need arises. AGILE has a security advisory board that can advise on issues involving any sensitive or potentially sensitive data. In WP3, each task leader is responsible for tracking the origin of the data.

To whom might your data be useful ('data utility'), outside your project?

In terms of utility, the tiered approach to analysing socio-technical systems – which will be further developed in WP – will be suitable for examining and mapping interdependencies and societal vulnerabilities to HILP events, depending on the user's preferences for resolution and level of detail. The advantage of the stress-test (ST) approach to be further developed in AGILE is its scalability: With analysis depth Tier 1, qualitative analyses of socio-economic systems and emergency response systems can be carried out quickly and cost-effectively. Tier 2 and Tier 3 depths of analysis also include quantitative approaches to uncover preparedness gaps, failure points, and cascading effects. If desired, very concrete simulations and recommendations from the scientific side can be made to policy makers and practitioners. The method, which will be comprehensively tested in the project with regard to its scientific quality, should then also be reliably applicable by other scientific institutions in cooperation with practitioners to increase the success rate of identifying and adequately monitoring fast developing risks into potential high-impact low-probability events in regions beyond the project's scope.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

Task leaders will strive to ensure that project-generated data can be safely shared publicly, and that all public datasets are deposited in a research data repository. Each dataset will be assigned a Digital Object Identifier (DOI) to enable citation and accessibility.

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

The chosen data repository must provide metadata for each dataset.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

To further aid their discoverability, keywords describing the datasets will be provided.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

Most research data repositories allow metadata of dataset to be harvested and indexed.

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

Repository which have the "CoreTrustSeal" certification will be considered trusted. Partners will make sure the data will be deposited in a trusted repository.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

If needed, we will make specific arrangements throughout the duration of the project to make sure data is deposited and accessible.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

The chosen data repository will provide a persistent identifier to each uploaded dataset.

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

We will not collect any personally identifiable information. If interviews/surveys are necessary, all data will be anonymized, and informed consent forms will be utilized to ensure that the data is non-personal and non-confidential, thus suitable and safe for publication. Data that is reused will be made openly available to the extent possible, taking into account the terms of use specified by each data source or any contractual obligations in force (e.g., restrictions on usage or publication). If for some reason data cannot be made openly available, it will be preserved by relevant task leaders at least for the duration of the project. We will abide by the license of different databases, and if data is obtained from project partners, we will consult them for license matters before publishing.

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

Discussion regarding embargo should be taking place at a project level when it deals with data shared between partner institutions. Such expectation, mostly valuable in the case of sensitive or confidential data sharing between partners, must be set out in the appropriate data sharing agreement if such agreements are needed.

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

Standardized and free access protocols to openly accessible data are ensured by trusted repositories.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

Each issuer of data is in charge of providing access during the project. We do not foresee publishing any confidential data containing private information. Therefore, we do not expect any restricted access to the published data.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

Checking the identity of people accessing the data is relevant when confidential data is to be made accessible to specific members of a WP (partners). Each institution sharing material oversees this to ensure that only the targeted member(s) of the partner institution will be granted access depending on the needs of the project.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

We do not foresee a need for anything like this for this work package.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

The trusted repositories will make the metadata openly available and licensed under a public domain dedication CC0, as per the grant agreement.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

Such features are provided by research data repositories.

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

Research material that can be made publicly available will be documented, including the information about the tools that are needed to work with the data, if needed. If possible,

software prototypes produced in the project will be made publicly available – unless publication exposes partners to confidentiality problems.

2.3. Making data interoperable:

What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

To the possible extent, the interoperability of the data will be supported by documentation in an open format.

2.3. Making data interoperable:

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

We plan to use the existing ontologies and vocabularies. If that is not possible, we will explain and provide documentation for the generated ontologies and vocabularies to allow reusing, refining, or extending them. This will be part of the dataset documentation. The AGILE project will also publish, as a result of work done in WP1, a list of definitions for terminology that may be used in other WPs and deliverables for this project.

2.3. Making data interoperable:

Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

Yes, relevant references will be included.

2.4. Increase data re-use:

How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

All documentation needed to validate data analysis and facilitate data re-use will accompany the data.

2.4. Increase data re-use:

Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

Each partner is in charge of ensuring that they can apply open licenses to material that is made publicly accessible.

2.4. Increase data re-use:

Will the data produced in the project be useable by third parties, in particular after the end of the project?

Yes, the goal is for the publicly available data to be available for everyone.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

The origin of the data will be documented as part of every scientific publication, following standards for citation format.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

All datasets which can be made publicly available will be recorded by the PI. The record will contain the name of the dataset, the issuer/owner/research team that produced it, a link to the data, and the license that is used.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

We will ensure that our storage solutions provide adequate security for the data (personal, confidential data), with sufficient storage space. We will follow the appropriate ethical protocols. We have specific guidelines for developing surveys and coding results, as well as for writing reports, to make sure it is not possible to track results and find who was the individual providing the answers to that specific survey. Not only surveys and their digital results are anonymized, but access to digital project folders is also restricted to people who have a contract with the relevant partner institutions.

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

We expect all deliverables to be in digital format or digitizable.

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

We will guarantee that all research outputs adhere to the FAIR principles. The quantity and quality of the data to be fed, the level of sensitivity, and how it will be processed, will be more precisely defined once the research environments are at a more advanced phase. The information still to be defined at a later stage includes the types of formats the project will collect or generate, the size of the data. During the project's duration, updates on the DPMs will be delivered to refine and/or specify any necessary protocols according to the project's requirements and research activities.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

The expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

These costs will be covered by the suggested budget.

Who will be responsible for data management in your project?

The data management is overseen by the coordinator of the project, who will mandate a specific partner as a main reference point for data related questions. Each task leader

together with the project management team will be responsible for data management in WP3.

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

We will preserve the data to the extent possible through trusted repositories. Any confidential data that cannot be made public will be preserved in private storage at least for the duration of the project.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

During the research project, all data will be stored on local servers. Only team members have access to the storage environment.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

Each partner oversees that confidential and personal data transfer between institutions is done in a lawful manner. However, we do not foresee the need to collect personal data, so we do not expect there to be any ethics issues that can have an impact on data sharing. Data that is reused will be made openly available to the fullest extent possible, taking into account the terms of use specified by each data source or any contractual obligations in force (e.g., restrictions on usage or publication).

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

When dealing with personal data, informed consent is always a requirement and a priority. Informed consent outlines what data is collected, where it is stored, and what is made public and what is deleted (if relevant). However, within WP3 we do not envision the collection of personal data.

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

FS has specific guidelines for developing surveys and coding results as well as for writing reports that ensure anonymity. Factor Social and its employees comply with Psychologists Ethical standards, and with the Portuguese Law 58/2019, which ensures the implementation of regulation regarding the protection of individuals with regard to the processing of personal data and the free movement of such data.
TUD is going to be in compliance with the TU Delft Research Data Framework Policy stating that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so. The project will be conducted in line with the Netherlands Code of Conduct for Research Integrity which contains a framework for good research practice.
Data management in UCL will comply with the UCL Research Data Policy. This policy ensures research data management aligns with the UK Data Protection Act (2018), European General Data Protection Regulation (2018).

Annex E:

Plan Overview

A Data Management Plan created using DMPonline
Title: AGILE: WP4
Creator: Rabea Schulz
Affiliation: European Commission
Funder: European Commission
Template: Horizon Europe Template

Project abstract:

This WP will create baseline scenarios (T4.1) that will be tested in the forseen case studies. It will implement:
9 STT1 assessing and managing risk and resilience for critical infrastructure (T4.2)
STT2s assessing cross-domain connectivity of systemic functions and expressing overall risk and resilience in the units of utility (T4.3)
STT3 revealing the impact of any disruption to critical functions enabling effective risk and resilience management plans to be developed (T4.4)
ID: 144499
Start date: 01-10-2023
End date: 30-09-2027
Last modified: 25-03-2024
AGILE: WP4

Data Summary

Will you re-use any existing data and what will you re-use it for?

T4.1: We may use data and documents on emergency management protocols, risk mitigation measures, and risk profiles to assist in generating the general scenarios.
T4.2: existing data (open-source or provided by stress test host) on topography, population, infrastructure, structure of local/regional emergency management and civil protection may be used to tailor the general scenario to the actual region. Personal data and contact data will be used to engage stakeholders, invite participants and arrange logistical matters.
T4.3: Existing data (open-source or provided by stress test host) on topography, population, infrastructure, structure of local/regional emergency management and civil protection may be used to tailor the general scenario to the actual region. We may use data and documents on emergency management protocols, risk mitigation measures, and risk profiles.
T4.4: Existing data (open-source or provided by stress test host) on topography, population, infrastructure, structure of local/regional emergency management and civil protection may be used to tailor the general scenario to the actual region. We may use data and documents on emergency management protocols, risk mitigation measures, and risk profiles, datasets of historical loss data, Vulnerability and fragility functions from partners and other EU projects, Hazard datasets, Existing Risk models, Exposure datasets, Socioeconomic loss data, Online database of empirical evidence of dynamics

and feedbacks of risk drivers, Existing Disaster Loss Databases, Equity data associated with spatiotemporal changes in exposure and vulnerability, Remote Sensing Data , Social Media Data, newspapers.

What types and formats of data will the project generate or re-use?

T4.1: Data will be collected through online desk-research. We may also re-use data from earlier project deliverables (particularly D1.1 and D1.2), to ensure that the scenarios are informed by opinions of experts in the field of risk and disaster reduction. Main formats: docx, pdf, jpeg, pptx, xlsx
General scenario data will be stored in the project's Sharepoint, accessible for the consortium. Any personal data will be stored in Sharepoint too, but in a folder with restricted access, only accessible for those needed (e.g. project management team and stress test host). Data for within the UCL team may be stored in space requested from UCL Research Data Storage Service.
T4.2: Re-use of maps, statistics about population and emergency response resources, organigrams, diagrams. This kind of data will be collected through online desk-research and/or provided through the case study host. Based on this, we will possibly create adapted maps to fit the scenario and/or create fictional fact-sheets related to the scenario, e.g. amount of people affected, damages, victims. These documents will be processed in the form of sharing and digitally editing in the preparation of the stress tests and printing them for the conduction. They may also be accessible by the participants via a cloud service or physical data drive during the stress test. main formats: docx, pdf, jpeg, pptx
Scenario data will be stored in the project's Sharepoint, accessible for the consortium. Personal data will be stored in Sharepoint too, but in a folder with restricted access, only accessible for those needed (e.g. project management team and stress test host).

T4.3: We plan to collect data from different stakeholders (e.g., infrastructure providers, citizens, local, regional and national authorities) in a two-day workshop in each case study. In the workshops, a mix of qualitative and quantitative data will be collected. We may collect list of participant, recording of the workshop session, transcript of conversation, and pictures of the workshops output. Whenever possible, we will use file formats suitable for long-term preservation and re-use of data. Quantitative data will be stored in .csv format and qualitative data and metadata will be stored in .txt format.
T4.4:
To ensure reusability and long-term preservation of research data, we plan to use commonly used formats (e.g., .cvs, .txt, .docx, .xlsx, .ipynb, etc.) as much as possible. We also plan to use NetCDF for climatic data, .tif data for satellite images, .shp for vectorial data.

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

T4.1: General scenarios will allow us to ensure we develop stress tests that capture some of the common challenges in HILP management. This will support stakeholders to develop a better understanding on how to prepare for and manage HILP events.
T4.2 aims to support stakeholders to develop a better understanding on how to prepare for and manage HILP. The tier 1 stress tests address the operational capacity on common points of failure. To conduct the stress tests, scenarios must be defined and potentially tailored to the host. Personal data must be collected to register and contact participants and stakeholders. The lessons learned form the starting point for the development of evidence-based planning approaches.
T4.3: This task allows us to capture the timescales of HILP events and identify key mechanisms pertaining to each phase (initial phase, response and recovery). The experiments will also serve to identify and evaluate risk mitigation or response options that will feedback into the living reference library as suggested options. The results will be translated into concrete guidelines for monitoring and decision-making for different HILP events and feed into the evidence-based planning.
T4.4: The purpose of data generation and re-use is the estimate of indicators for hazard, exposure, vulnerability, previous impacts and, wherever possible, recovery information in the stress test area. We also plan to use these information to model relationships between different indicators, in order to create insight into cascading mechanisms pertaining to each phase (initial phase, response and recovery). The results will be translated into concrete guidelines for monitoring and decision-making for different HILP events and feed into the evidence-based planning.

What is the expected size of the data that you intend to generate or re-use?

T4.1: Overall, we expect to generate no more than 250GB of data. For data storage, space will be requested through the UCL Research Data Storage Service, which can store up to 1TB of data. For sharing with the AGILE consortium, the expected amount of data can be stored in the project's Sharepoint.
T4.2: scenario data max. a single-digit amount of GB per stress test; personal data/contact data less than a GB. This amount of data can be stored in the project's Sharepoint. Data that should not be shared with anyone outside of the Coordinator, data can also be stored on local servers.
T4.3: We expect that the size of the collected data will be less than 250 GB. We plan to request storage space from TU Delft OneDrive. In the case of confidential information, we can utilize the project storage of TU Delft.
T4.4: We expect that the size of the collected data will be less than 1 TB.

What is the origin/provenance of the data, either generated or re-used?

T4.1:
T4.2: scenario data: public websites, maps providers and open data bases, stress tests hosts (organisations, authorities within the consortium)
T4.3: Data for this task will be collected from stakeholders' workshops.
T4.4: Data for this task will be collected from local authorities and research centres, scientific literature and possibly grey literature, satellite images.

To whom might your data be useful ('data utility'), outside your project?

T4.1: The data may be useful for academics, researchers in the field of crisis decision making. The scenarios will also be useful to those involved in the practical side of crisis management, business continuity, and organisational resilience. The general scenarios may be useful for other authorities, organisations, projects and individuals in risk management and civil protection as a basis for own trainings, exercises or stress tests.
T4.2: scenario data and information about the implementation of tier 1 may be useful for other authorities, organisations, projects and individuals in risk management and civil protection as a basis for own trainings, exercises or stress tests. Lessons learned and related guidelines will be published through WP5.
T4.3: The data may be useful for academics, researchers in the field of crisis decision making. It may also be useful for developing guidelines and also for authorities, organizations, projects and individuals in risk management and civil protection.
T4.4: The data may be useful for academics, researchers in the fields of crisis decision making, environmental science, geology, resilience studies . It may also be useful for developing guidelines and also for authorities, organizations, projects and individuals in risk management and civil protection. They may inform local authorities on how to improve resilience of the studied system.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

T4.1: Stress test partners may share data related to resources, capacities, and gaps that should remain confidential within the consortium and the case study partner's organisation/authority. Therefore, only general case study scenarios and evaluation reports will be published as WP deliverables. The WP deliverables will receive a DOI when uploaded in CORDIS.
T4.2: only the deliverable will receive a DOI when uploaded in CORDIS. Personal data will not be published.

T4.3: All datasets will be assigned a Digital Object Identifier (DOI), to make them citable and persistently available. We will use appropriate data repositories like Zenodo or 4TU Research data for uploading and storing the data. We will ensure that no confidential data that contains private information is published.
T4.4: All publishable data will be uploaded on a trusted repository (e.g. Zenodo), which assigns a DOI. the deliverable will receive a DOI when uploaded in CORDIS. Personal data will not be published.

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

T4.1: It is not expected that this will be required for this task.
T4.2: not foreseen for this task

T4.3: All publishable data will be made openly available through Zenodo or 4TU.ResearchData, a trusted and certified data repository. All datasets will be accompanied by rich metadata, adhering to the DataCite Metadata Standard, to ensure that they are findable.
T4.4: The chosen data repository must provide metadata for each dataset.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

T4.1: No metadata foreseen for this task
T4.2: no metadata foreseen for this task
T4.3: All publishable data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU.ResearchData. To further aid their discoverability, keywords describing the datasets will be added.
T4.4: yes

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

T4.1: No metadata foreseen for this task
T4.2: no metadata foreseen for this task

T4.3: Both Zenodo and 4TU.Research Data make metadata available under CC0 license such that it can be harvested.
T4.4: yes

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

All: Personal data as well as confidential data provided by the stress test hosts will not be deposited in a public repository.
T4.1: During the project, scenario data and the evaluation of stress tests will be stored in the project internal Sharepoint repository. The general case study scenarios and evaluation reports will be submitted to the EC and published on CORDIS. Document packages with scenario data may become part of the projects website or the database to be developed in WP2, but that is not decided yet. Personal data and contact data will not be stored in a public repository.

T4.2: during the project, scenario data and the evaluation of stress tests will be stored in the project internal Sharepoint repository. The Evaluation report will be submitted to the EC and published on CORDIS. Document packages with scenario data may become part of the projects website or the data base to be developed in WP2, but that is not decided yet.
T4.3: All data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU. Research Data, both trusted and certified data repositories. Both repositories have CoreTrustSeal certification. All the data will have DOI for persistent identification and will be stored for at least 10 years.
T4.4: during the project, data will be stored in the project internal Sharepoint repository, and in G-Drive. We will use a trusted repository (e.g. Zenodo) to upload all the publishable datasets. Personal data and contact data will not be stored in a public repository.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

T4.1: N/A
T4.2: no
T4.3: We will make specific arrangements to make sure the collected data during the workshops is archived. We can upload up to 1 TB per year in 4TU research data repository. This is made available by TU Delft for its employees. We will figure out this throughout the duration of the project.
T4.4: no

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

T4.1: CORDIS provides every uploaded document with a DOI
T4.2: CORDIS provides every uploaded document with a DOI
T4.3: All data resulting from the project except for confidential data with private information will be made openly available through Zenodo or 4TU.ResearchData. Both repositories ensure DOIs for datasets.
T4.4: we will use trusted repositories (e.g. Zenodo) that provide every uploaded document with a DOI.

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

General: No personal data will be made openly available. If data provided by case study hosts is subject to confidentiality, it will not be published.

T4.1: The general case study scenarios and the Evaluation Reports will be openly available. It is possible that information of the stress testing scenarios will become part of the public database, but this is to be confirmed.
T4.2: the Evaluation Report will be openly available; possibly, the general scenarios will become part of the public database, but to be confirmed
T4.3: We plan to collect data from different stakeholders in the workshops. No confidential data containing private information will be made openly available. Anonymous data from workshops as well as description of the workshop protocol will be made accessible to the public.
T4.4: no personal data will be shared. Publishable data may be shared on a trusted repository (e.g. Zenodo).

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

T4.1: N/A
T4.2: n/a
T4.3: We do not expect any embargo period for the data that we plan to make openly available through trusted repositories.
T4.4: We do not expect any embargo period for the data that we plan to make openly available through trusted repositories.

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

T4.1: The general case study scenarios and Evaluation Reports will be accessible through CORDIS, which provides a free and standardized access protocol.
T4.3: Yes, this will be provided by the trusted repositories we have identified.
T4.4: Yes, this will be provided by the trusted repository.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

T4.1: Access to personal data and contact data will be restricted to the persons that need access for implementing the stress test (project management team and the host), restricted access will be provided through dedicated, restricted folders in Sharepoint (and possibly also through UCL's Research Data Storage Service if just within the UCL team).
T4.2: access to personal data and contact data will be restricted to the persons that need access for implementing the stress test, so project management team and the host; restricted access will be provided through dedicated, restricted folders in Sharepoint
T4.3: We will not publish any confidential data containing private information. Therefore, we do not expect any restricted access to the published data.

T4.4: We will not publish any confidential data containing private information. Therefore, we do not expect any restricted access to the published data.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

T4.1: We will follow security protocol to access the data during the project. This will include a personal login to access data stored in UCL's Research Data Storage service and login to Sharepoint with 2 factor authentication. The case study scenarios and evaluation Report will be publicly available as per the project deliverables.
T4.2: login to Sharepoint with 2 factor authentication
T4.4: login to Sharepoint with 2 factor authentication. Login to G-Drive. The trusted repository will have its security protocols

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

T4.1: A need for this is not anticipated. However, if any data is deemed sensitive, advice of the AGILE project's security advisory committee will be sought before sharing of this data.
T4.2: no
T4.3: We will be collecting identifiable information. At the conclusion of the project, an anonymized version of this data will be made available. If partners request access to the personal data, we will consult with the TU Delft support team and the project coordinator to ensure compliance with GDPR regulations.
T4.4: no need for data access committee

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

T4.1: As covered above, only the case study scenarios and Evaluation Reports will be made openly available.
T4.3: The trusted repositories will make the metadata openly available and licensed under a public domain dedication CC0, as per the grant agreement.
T4.4: We will use a repository that will make the metadata openly available and licensed under a public domain dedication CC0, as per the grant agreement.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

T4.1: As covered above, only the The case study scenarios and Evaluation Reports will be made openly available. These will remain available as long as CORDIS permits.
T4.3: We will preserve all data that can be openly shared for a minimum of 10 years, making it accessible to everyone. The trusted repositories guarantee the preservation of the metadata after the data is no longer available.
T4.4: Such features are provided by research data repositories.

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

T4.1: As covered above, only the case study scenarios and Evaluation Reports will be made openly available. If any additional data is published for stress testing scenarios, it is expected to be text data. Therefore, we do not anticipate a need for this.
T4.2: N/A
T4.3: All published datasets will have the necessary documentation containing the description of the tools to re-run the experiment ensuring reproducibility.
T4.4: All published datasets will have the necessary documentation containing the description of the tools to re-run the experiment ensuring reproducibility. Codes will be properly commented and wrote according to best practices. The publication of software is still to be confirmed.

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

T4.1: As covered above, only the case study scenarios and Evaluation Reports will be made openly available. The AGILE project will also publish a list of definitions (as part of deliverable 1.1) for terminology that may be used in these documents. Other than this, there is no anticipated need for vocabularies, standards, formats or methodologies for interpretation of any published data.
T4.3: We do not have metadata standards to describe workshops output. Instead we will provide the documentation in a form of README file.
T4.4: Each dataset will include metadata that will describe and document the data. Whenever necessary, a readme file will be created.

2.3. Making data interoperable:

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

T4.1: As covered above, only the case study scenarios and Evaluation Reports will be made openly available. The AGILE project will also publish a list of definitions (as part of deliverable 1.1) for terminology that may be used in this report.
T4.3: We do not have metadata standards to describe workshop output. instead we will provide the documentation in a form of README file.
T4.4: We do not expect to use uncommon or generate project specific ontologies or vocabularies.

2.3. Making data interoperable:
Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

T4.1: Any relevant references will be included in the case study scenarios and evaulation reports.
T4.2: probably not
T4.3: Yes, relevant references will be included in the metadata of the datasets and associated publication.
T4.4: Yes, relevant references will be included in the datasets and associated publications.

2.4. Increase data re-use:
How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

T4.1: As covered above, only the case study scenarios and Evaluation Reports will be made openly available. It is not anticipated that any additional documentation will be necessary to facilitate data re-use.
T4.3: All documentation needed to validate data analysis and facilitate data re-use will accompany the data via a README file created in accordance with the 4TU.ResearchData guidelines.
T4.4: All documentation needed to validate data analysis and facilitate data re-use will be included in the codes or accompany the data via a README file .

2.4. Increase data re-use:

Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

T4.1: As covered above, only the case study scenarios and Evaluation Report will be made openly available (through CORDIS).
T4.3: Yes, we will find open license for all the datasets. All material will have CC-Like license ensuring free availability in the public domain and widest possible re-use, in line with the grant agreement.
T4.4: we will use open license for datasets

2.4. Increase data re-use:

Will the data produced in the project be useable by third parties, in particular after the end of the project?

T4.1: To be confirmed for scenario data as this would be tailored to the stress test host; the general case study scenarios will be published as D4.1
T4.2: to be confirmed for scenario data as this would be tailored to the stress test host; the general case study scenarios will be published as D4.1
T4.3: Yes, we will make all the data except for confidential ones containing private information available to all.
T4.4: Yes, we will make all the data except for confidential ones containing private information available to all.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

T4.1: As above, it is expected that only the general case study scenarios and Evaluation Reports will be made publicly available beyond the AGILE team as a result of this WP. If the decision is made to publish any specific scenario data, then yes, the provenance of the data be thoroughly documented using the appropriate standards (see more detail in section 2.3).
T4.3: Yes, see section 2.3.
T4.4: Yes, see section 2.3.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

T4.1: The UCL team has extensive experience regarding data quality assurance processes. The team will call upon the support offered by UCL's Research Data services if necessary. If any sensitive data is shared during this work package, the security advisory board for the AGILE project will be consulted on if/how to best store and utilise this data.

T4.3: We will rely on the best practices on the domain and call on the data support team at TU Delft. In case of doubt regarding the confidentiality of the data sets we will seek advice from the security advisory board of the project.
T4.4: We will rely on the best practices on the domain , including a throughout data analysis and outlier detection.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

T4.1: An application will be made for ethics approval from the ethics committee of UCL's Institute for Risk and Disaster Reduction. Data storage within the AGILE consortium and within the UCL team specifically is done to high levels of security (e.g. two-factor authentication). If any sensitive data is shared during this work package, the security advisory board for the AGILE project will be consulted on if/how to best store and utilise this data.
T4.3: We will conduct workshops, which will be reviewed by the TU Delft Ethics Committee. We will ensure that no personal data is made available without the consent of the respondent. We do not expect any data security concerns for this work package.

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

T4.1: We expect outputs to be digital
T4.2: N/A
T4.3: We expect all outputs to be digital as per section 1.
T4.4: We expect all outputs to be digital

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

T4.1: We will ensure that all publicly available research outputs are FAIR.
T4.2: N/A

T4.3: We will ensure that all publicly available research outputs are FAIR.
T4.4: We will ensure that all publicly available research outputs are FAIR.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

T4.1: Storage in the UCL repository is covered by UCL. Storage on Sharepoint is provided through ARTTIC - costs related to the project unknown, please see WP6; publication of project results on CORDIS without costs
T4.2: storage on Sharepoint provided through ARTTIC - costs related to the project unknown, please see WP6; publication of project results on CORDIS without costs
T4.3: The expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.
T4.4: The expected costs for making data and other research outputs FAIR have been accounted for in the AGILE budget.

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

T4.1: Costs will be covered by the suggested budget.
T4.2: N/A
T4.3: These costs will be covered by the suggested budget.
T4.4: These costs will be covered by the suggested budget.

Who will be responsible for data management in your project?

T4.1: Task Leader together with Project Management Team
T4.2: Task Leader together with Project Management Team
T4.3: Any questions related to data management should be directed to the work package leader, who will then guide us to the appropriate contact person
T4.4: Task Leader together with Project Management Team

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

T4.1: Data will be kept for the duration stated in the Grant Agreement
T4.2: Data will be kept for the duration stated in the Grant Agreement

T4.3: We will preserve the data to the extent possible through the trusted repositories. Any confidential data that cannot be made public will be preserved in private storage at least for the duration of the project.
T4.4: We will preserve the data to the extent possible through the trusted repositories. Any confidential data that cannot be made public will be preserved in private storage at least for the duration of the project.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

T4.1: We will use UCL's Research Data Storage Service, where data is fully backed-up daily. Specialist technical support is available to help with using this service.
Data that does not contain any personal details will be shared within the project Sharepoint. If sensitive, approval will be sought from AGILE's security advisory board before sharing with the wider consortium. The sharepoint repository is only accessible with 2 Factor Authentication, laptops/computers/mobile devices are secured by password; oldes versions of a document can be recovered through Sharepoint's version control; deleted documents can be restored from the trash folder within Sharepoint.
T4.2: Sharepoint repository is only accessible with 2 Factor Authentication, laptops/computers/mobile devices are secured by password; oldes versions of a document can be recovered through Sharepoint's version control; deleted documents can be restored from the trash folder within Sharepoint. Personal and confidential data will be stored in folders with dedicated access rights on a needs-basis.
T4.3: We will use TU Delft approved storage solution, where data is backed up automatically.
During the course of the research project, all data will be stored on local servers maintained and automatically backed up by TU Delft ICT. Every night the data will be automatically backed up. The data will be replicated over multiple sites/data centers. Data can be recovered with the help of TU Delft ICT services in the event of an incident.
Only team members have access to the designated server, limited to the principal investigator of the project (Prof. Tina Comes), and Dr. Nazli Yonca Aydin. The storage security is ensured by TU Delft ICT services.
The Faculty Data Steward will provide additional advice, as needed, on data storage during the research project. This data storage solution offers secure storage and transfer. After the end of the project, all datasets will be published in Zenodo or 4TU.ResearchData. The data will be openly accessible to all.
T4.4: Sharepoint repository is only accessible with 2 Factor Authentication, G-Drive repository requires authentication, laptops/computers/mobile devices are secured by password; older versions of a document can be recovered through Sharepoint or G-Drive version control; deleted documents can be restored from the trash folder within Sharepoint. To publish data we will use a trusted repository.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

T4.1: If necessary, an ethics application will be made to the ethics commitee of UCL's Institute for Risk and Disaster Reduction in advance of this task.

T4.4 AGILE has set up Ethics Focal Points which will be asked to provide feedbacks any matter should arise.

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

T4.1: Where participants are involved in WP activities, they will be provided with a participant information sheet that details how data will be handled prior to participation. Only with their approval will activities proceed.
T4.2: yes
T4.3: For the workshops, we expect to collect personal data. Long term preservation strategy for the collected data will be presented to the participants and subject to their approvals.
T4.4 yes

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

T4.1 Data management will comply with the UCL Research Data Policy. This policy ensures research data management aligns with the UK Data Protection Act (2018), European General Data Protection Regulation (2018).

T4.3: We are going to be in compliance with the TU Delft Research Data Framework Policy stating that research data, code and any other materials needed to reproduce research findings are appropriately documented and shared in a research data repository in accordance with the FAIR principles (Findable, Accessible, Interoperable and Reusable) for at least 10 years from the end of the research project, unless there are valid reasons not to do so.
The project will be conducted in line with the Netherlands Code of Conduct for Research Integrity which contains a framework for good research practice.

T4.4 CMCC Compliance Office is in charge of privacy and personal data management in compliance with EU rules. Compliance office is in charge of implementing the Foundation rules on processing personal data within the context of projects and scientific research activities (this also applies to human participation in research).
CMCC has appointed Mr. Andrea Lisi as External Data Protection Officer (DPO): his role is to ensure that CMCC processes personal data in compliance with the GDPR, other applicable data protection rules and also performance of other privacy-related issues.

Annex F:

Plan Overview

A Data Management Plan created using DMPonline

Title: AGILE WP 5

Creator:vlatko jovanovski

Affiliation: Other

Funder: European Commission

Template: Horizon Europe Template

Project abstract:
This work package will build on the results of the previous work packages (1,2,3 and 4) and will translate their results into harmonized approaches for the management of HILP risks and events on a more operational level. WP5 will work towards the uptake and standardization of the AGILE Stress Test toolkit and related planning tools. By designing critical steps and research questions the work package will provide an innovative paper-based tool supporting evidence-based planning for HILP events. This tool will support first responders and relevant organizations to plan for emergency response during HILP events. Furthermore a desk study on most needed skills and knowledge for successful HILP response will be introduced. Key informants will be interviewed including actors in previous HILP events and a selection of expert academia. Information of these interviews will be collected and analysed to bring forth current best practices and challenges of capability development during HILP events. Based on the gap & needs analysis from the case studies structured modular capacity development guidance will be developed and tested. The analysis from the gaps and challenges will also feed the process of development of the guidelines and collection of best practices for effective risk and crisis communication around HILP events. The ultimate goal with this task is to enhance individual and community preparedness and reduce unfit behaviors during HILP crisis. In particular, risk communication messages will be tested to understand which are the most effective for enhancing preparedness.

ID: 147135

Last modified: 14-03-2024

AGILE WP 5

Data Summary

Will you re-use any existing data and what will you re-use it for?

We plan to collect data from different project partners and open sources such as HDX, Copernicus, NASA, Our World in Data, etc. The collected data will be used to develop the guidelines for evidence-based planning of HILP events, identification of the needed skills

and knowledge for managing HILP events and the guidelines on risk communication during HILP events.

What types and formats of data will the project generate or re-use?

We plan to conduct a survey of the stakeholders involved in this project (project partners and case study entities). In the survey, a mix of qualitative and quantitative data will be collected. The objective for the data collection is to understand the requirements for the HILP evidence based planning, capacity development and risk communication. We will also collect data from open access data sources like HDX, Copernicus, NASA, Our World in Data, etc. Whenever possible, we will use file formats suitable for long-term preservation and re-use of research data. Quantitative data will be stored in .csv format and qualitative interviews and metadata will be stored in .txt format.

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

There are two purposes. First, we will conduct a survey of the stakeholders to understand base line status with evidence based planning for HILP events, capacity development and risk communication. Second, we will collect data from open access data sources like HDX, Copernicus, NASA, Our World in Data, etc., to develop the proposed guidelines and tools.

What is the expected size of the data that you intend to generate or re-use?

We expect the collected data to size between 250 GB and 1 TB

What is the origin/provenance of the data, either generated or re-used?

Data for this WP will be collected from stakeholders' survey and open access data sources such as HDX, Copernicus, NASA, Our World in Data, etc. Specific attention will be given to the license under which the data is distributed. The protocol to obtain data will be established before the transfer takes place

To whom might your data be useful ('data utility'), outside your project?

The collected data will be useful for academics, researchers in the field of disaster resilience and practitioners. It will also be useful for public policy making.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

All datasets will be assigned reference numbers to make them citable and persistently available. We will use appropriate data repositories for uploading and storing the data. We will ensure that no confidential data that contains private information is published.

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

All data will be made openly available through a trusted and certified data repository. All datasets will be accompanied by rich metadata, adhering to the DataCite Metadata Standard, to ensure that they are findable.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

All data resulting from the project except for confidential data with private information will be made openly available. To further aid their discoverability, keywords describing the datasets will be added.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

The data repository system in use will allow metadata to be available and harvested.

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

All data resulting from the project except for confidential data with private information will be made openly available through trusted and certified data repositories.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

We will make specific arrangements to make sure the whole database is archived. We will figure out this throughout the duration of the project.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

All data resulting from the project except for confidential data with private information will be made openly available.

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

We plan to collect data from different project partners and open sources such as HDX, Copernicus, NASA, Our World in Data, etc. We will abide by the license of different

databases. No confidential data containing private information will be made openly available. If the data is obtained from the project partners, we will consult them for license matters before publishing.

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

We do not expect any embargo period for the data that we plan to make openly available through trusted repositories.

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

Yes, this will be provided by the trusted repositories we have identified.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

We will not publish any confidential data containing private information. Therefore, we do not expect any restricted access to the published data.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

We will ensure the integrity of the database by providing a secure and safe environment through dedicated log-ins. To implement this, we will seek help from IT and legal experts associated with PPI.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

We do not foresee a need for anything like this for this work package.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

The trusted repositories will make the metadata openly available and licensed under a public domain dedication as per the grant agreement.

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

We will preserve the data for at least 10 years for everyone. The trusted repositories guarantee the preservation of the metadata after the data is no longer available.

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

All datasets will have the necessary documentation containing the description of the tools to re-run the experiment ensuring reproducibility.

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

We plan to collect data from HDX database. HDX has metadata standards. We will abide by that standard for the all the datasets.

2.3. Making data interoperable:
In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

We plan to use the existing ontologies and vocabularies. If that is not possible, we will explain the generated ontologies and vocabularies to allow reusing, refining, or extending them. This will be part of the dataset documentation.

2.3. Making data interoperable:
Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

Yes, relevant references will be included in the metadata of the datasets.

2.4. Increase data re-use:

How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

All documentation needed to validate data analysis and facilitate data re-use will accompany the data via appropriate file creation.

2.4. Increase data re-use:
Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

Yes, we will find open license for all the datasets. All material will have CC-Like license ensuring free availability in the public domain and widest possible re-use, in line with the grant agreement.

2.4. Increase data re-use:
Will the data produced in the project be useable by third parties, in particular after the end of the project?

Yes, we will make all the data except for confidential ones containing private information available to all.

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

Yes, see section 2.3.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

We will rely on the best practices on the domain.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

We will ensure that no personal data is made available without the consent of the respondent. We do not expect any data security concerns for this work package

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

We expect all outputs to be digital as per section 1.

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

We will ensure that all publicly available research outputs are FAIR.

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

Including storage, an amount of estimated 3000, -€ in total will be needed for this operation.

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

These costs will be covered via the allocated budget.

Who will be responsible for data management in your project?

Persons responsible for the data management for AGILE WP5 are Albrecht Beck and Vlatko Jovanovski.

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

We will preserve the data to the extent possible through the trusted repositories. Any confidential data that cannot be made public will be preserved in private storage at least for the duration of the project.

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

We will use PPI approved storage solution, where data is backed up automatically. During the course of the research project, all data will be stored on local servers maintained and automatically backed up by PPI. Data will be recovered with the help of PPI ICT services in the event of an incident.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

Any research protocol involving humans will be reviewed by PPI Core Management.

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

For the survey, we expect to collect personal data. Long term preservation strategy for the collected data will be presented to the participants and subject to their approvals.

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

No we are not going to use additional procedures for data management.

Annex G:

Plan Overview

A Data Management Plan created using DMPonline
Title: AGILE - WP6
Creator: Andreas Seipelt
Affiliation: Other
Funder: European Commission
Template: Horizon Europe Template

Project abstract:

Agnostic risk management for high Impact Low Probability events
ID: 144167
Start date: 01-10-2023
End date: 30-09-2027
Last modified: 25-03-2024
Grant number / URL: 101121356
AGILE - WP6

Data Summary

Will you re-use any existing data and what will you re-use it for?

In WP6, we aim to harness the existing data sources wherever it is possible to strengthen our stakeholder engagement and sustainability planning. This involves gathering information from the consortium partners and communicating via social media and the CMINE platform. Through this approach, we will shape our stakeholder mapping and engagement strategy by gaining valuable insights into the preferences, needs and expectations of diverse stakeholders in the context of HILP events. This will significantly support the objectives of WP1 to WP5. In addition, existing data collected from databases focusing on civil security, crisis management, or related topics, may provide additional insights or opportunities for collaboration.
Specifically this will entail:
Text and images from project work plan, and from (scientific as well as general interest) publications arising from the project
Personal data for the subscription of newsletters and invitation to AGILE public events originating from ARTTIC contacts database

What types and formats of data will the project generate or re-use?

- · Text and images in standard processable data formats, e.g. .doc(x), .ppt(x), .txt, .jp(e)g, .ai, .psd, up to 5 GB total
- · Reports, documents, pictures, tables, presentations: approx.. 50GB (format .doc, .xls, .jpg, .pdf, .ppt)

- · Personal data for the subscription of newsletters and invitation to AGILE public events

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

The purpose of data generation or re-use is to engage with stakeholders about the project communication, dissemination, and exploitation efforts. By analyzing data on stakeholder preferences, engagement metrics, and collaboration opportunities, we tailor strategies to effectively involve stakeholders, optimize communication channels, and identify exploitation opportunities. This ensures the project's outcomes reach relevant stakeholders and maximize its impact.

What is the expected size of the data that you intend to generate or re-use?

Text and images in standard processable data formats, e.g. .doc(x), .ppt(x), .txt, .jp(e)g, .ai, .psd, up to 5 GB total
· Reports, documents, pictures, tables, presentations: approx.. 50GB (format .doc, .xls, .jpg, .pdf, .ppt)

What is the origin/provenance of the data, either generated or re-used?

It is a combination of internally generated materials (pictures, posters, flyers, videos and other communication materials) specific to the AGILE project and also some externally collected information (surveys, existing databases, or literature reviews) used to supplement the project activities.

To whom might your data be useful ('data utility'), outside your project?

Consortium members for exploitation, members of the Project Advisory Board and the broader AGILE stakeholder community to explore future collaboration and development options.
All the project stakeholders impacted by the communication

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

Data will be hosted and made findable within the consortium through the collaborative workspace created by ARTTIC and controlled by the PMO. It will contain open and confidential data produced within AGILE. This data will be made findable through an organised structure with specific sections sorted by topics where the data can be shared,

discussed and used to amplify the project's ambitions. Each document must be identified with a unique filing code, regardless of the document title, file names and referencing conventions that each partner might use in local archives.
For deliverables, the file name must start with AGILE and contain the following elements as a minimum:
AGILE_Dnumber_Short-Title_VersionNumber
Example: AGILE_D1.6_Imp_Strgy_V1.0.pdf

For all other project documents, the file name must start with AGILE and contain the following elements as a minimum:
AGILE_Type_Title_VersionNumber
Example: AGILE_AGD_KOM_V1.0.doc

Where:
AGILE: the project acronym
AGD: Type of document. In this case, it is the Agenda
KOM: title of the document. In this case, it is to specify that the Agenda is related to the kick-off meeting
Vx.y: the versioning number (e.g. V0.1, V0.2, V1.0, V1.1)

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

not applicable

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

not applicable

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

not applicable

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

All data will be hosted and made findable within the consortium through the collaborative workspace (SHP) created by ARTTIC and controlled by the PMO.

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

We will store data on the project collaborative workspace (SHP) in an organised structure with specific sections sorted by topics within each WPs.

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

not applicable

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

Personal data will not be made publically accessible, but all public project materials (deliverables, poster, leaflets, etc..) will be made available through the AGILE website (https://www.project-agile.eu/).

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

not applicable

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

not applicable

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

not applicable

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

not applicable

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

not applicable

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

not applicable

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

not applicable

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

not applicable

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

not applicable

2.3. Making data interoperable:

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

not applicable

2.3. Making data interoperable:
Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

not applicable

2.4. Increase data re-use:
How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

not applicable

2.4. Increase data re-use:
Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

All the public accessible materials as per the GAM will be made available through the AGILE project website.

2.4. Increase data re-use:
Will the data produced in the project be useable by third parties, in particular after the end of the project?

not applicable

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

not applicable

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

For all data created as part of the AGILE project, there is a clear filing structure (name of folders, versioning and quality assurance processes) supported by the AGILE Project Management Office (PMO). Clear procedures to systematically archive all AGILE documentation are in place.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

not applicable

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

not applicable

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

not applicable

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

No specific costs are expected related to the storage of the data generated in WP6

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

see above

Who will be responsible for data management in your project?

Johanniter-Unfall-Hilfe e.V. (Project Coordinator)

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

not applicable

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

The AGILE project is fully implemented within the EU General Data Protection Regulation (GDPR) which entered in application on the 25th May 2018 and replaced the Data Protection Directive 95/46/EC. Specific care is taken for dissemination activities, e.g. the AGILE public website.
Storage and backup for all AGILE project documentation is ensured via SharePoint set-up by PMO, which has the appropriate back-up systems in place. Further, SharePoint is protected by password and AES 256-bit encryption.

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

not applicable

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

Informed consent for data sharing and long-term preservation will be included in questionnaires dealing with personal data. Participants will be asked to provide consent for the sharing and preservation of their personal information, specifying the purposes for which the data will be used, shared, and preserved. The personal information will not be shared. Consent forms will be collected from each partner involved in the project, and stakeholders will provide consent via the AGILE website when registering their information to participate in the project. All collected information will be securely stored in the AGILE SHP and will be password-protected.

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

not applicable

Annex H:

Plan Overview

A Data Management Plan created using DMPonline
Title: AGILE: WP7 and WP8
Creator: Gordana Cveljo
Affiliation: Other
Funder: European Commission
Template: Horizon Europe Template

Project abstract:

This task ensures and supports effective planning, implementation, coordination, realisation of the project activities, by coordinating the joint efforts of the consortium during the execution of the project by the fulfilment of the consortium's contractual obligations, and ensuring the smooth progress of the work plan and day-to-day project management. It is carried out in close collaboration with the Steering Committee (all WPL
are members) and the General Assembly.
ID: 144146
Start date: 01-10-2023
End date: 30-09-2027
Last modified: 01-03-2024
AGILE: WP7 and WP8

Data Summary

Will you re-use any existing data and what will you re-use it for?

WP7: Personal data, e.g. contact details (name, email addresses, organisations name, phone number) of consortium partners and the project advisory board are used. They are used for mail exchange, mailing lists, information distribution, invitation to meetings etc. They are stored in the common workspace Sharepoint. Furthermore, contractual and financial details of the Grand Agreement will be used for the implementation of the project and for technical and financial planning and reporting as required by the European Commission.

WP8: For creating D8.1 personal data incl. CV of the two ethics focal points and the public information about the relevant (ethical) structures within TU Delft and CMCC were used. This was shared with the EU Commission.
If needed for further definition of AGILE's approach for the management of ethics issues existing ethical guidelines or policies of project partners or other institutions (available online) may be used. If so, they might be send to all partners with practical guidelines for use.

What types and formats of data will the project generate or re-use?

WP7: Deliverables are and will be generated as administrative input, the type is a report (docx, pdf). Internal documents and presentations will be created (docx, pdf, pptx, xlsx).
WP8: The Deliverables D8.1 is an already created report in the format docx and pdf. In this WP may reports, guidelines, ethics issue register in the formats docx, pdf, xlsx be created.

What is the purpose of the data generation or re-use and its relation to the objectives of the project?

WP7: The re-use of data is for fulfilling the objectives as a project coordinator, e.g. coordinating, planning and monitoring the implementation of the project in constant exchange with all project partners and external stakeholders. The Reports generated are to fulfill the obligations in the Grant Agreement, mostly as deliverables.
WP8: The personal data and CVs were used to fulfill the requirement of two Ethics Focal Points and for the definition of processes regarding ethics issues, as requested by the Commission. If ethical issues arise, the will be reported, registered and documented to ensure compliance with the ethical requirements that is set out in the Grand Agreement.

What is the expected size of the data that you intend to generate or re-use?

WP7: The re-use of personal data is less than a GB. The creation of reports, presentations, register we expect to be max. a single digit amount of GB.

WP8: The guidelines, issue reports and register is less than a GB.

What is the origin/provenance of the data, either generated or re-used?

WP7: Data for this WP comes from the consortium partners, the project advisory board members and potential external stakeholders, as well as from the Grant Agreement. For the creation of deliverables, input from other projects may be consulted via CORDIS or project websites.
WP8: The data from the consortium partners incl. the ethics focal points as well as openly available information from the websites of TU Delft and CMCC is used. Guidelines might be generated based on input from the AGILE Security Advisory Board, the AGILE Ethics Focal Points as well as ethics deliverables of other projects that are available on CORDIS. If ethics issues arise, they will be reported by project partners.

To whom might your data be useful ('data utility'), outside your project?

WP7: Personal data and contact data are only useful and provided within the project/consortium. The coordination deliverables may be useful for coordinators of other projects.
WP8: D8.1 was categorized as "sensitive" by the Commission, e.g. no access to it outside the project. Based on that, the documentation of ethics issues will also not be public.

FAIR data

2.1. Making data findable, including provisions for metadata: Will data be identified by a persistent identifier?

WP7: The WP deliverables are automatically allocated with a DOI when uploaded on CORDIS.
WP8: No.

2.1. Making data findable, including provisions for metadata: Will rich metadata be provided to allow discovery? What metadata will be created? What disciplinary or general standards will be followed? In case metadata standards do not exist in your discipline, please outline what type of metadata will be created and how.

WP7: No.
WP8: No.

2.1. Making data findable, including provisions for metadata: Will search keywords be provided in the metadata to optimize the possibility for discovery and then potential re-use?

WP7: No.
WP8: No.

2.1. Making data findable, including provisions for metadata: Will metadata be offered in such a way that it can be harvested and indexed?

WP7: no
WP8: no

2.2. Making data accessible - Repository: Will the data be deposited in a trusted repository?

WP7: The data will be stored in CORDIS.
WP8: N/A

2.2. Making data accessible - Repository: Have you explored appropriate arrangements with the identified repository where your data will be deposited?

WP7: no
WP8: no

2.2. Making data accessible - Repository: Does the repository ensure that the data is assigned an identifier? Will the repository resolve the identifier to a digital object?

WP7: CORIDS automatically assign a DOI to each deliverable.
WP8: n/a

2.2. Making data accessible - Data:
Will all data be made openly available? If certain datasets cannot be shared (or need to be shared under restricted access conditions), explain why, clearly separating legal and contractual reasons from intentional restrictions. Note that in multi-beneficiary projects it is also possible for specific beneficiaries to keep their data closed if opening their data goes against their legitimate interests or other constraints as per the Grant Agreement.

WP7: The deliverables are planned to be shared openly, due to the Grant Agreement. The personal data is sensitive and is therefore not openly available.
WP8: The deliverable D8.1 has been deemed as "sensitive" by the Commission, therefore it is not public, so other documents associated with this will also not be public.

2.2. Making data accessible - Data:
If an embargo is applied to give time to publish or seek protection of the intellectual property (e.g. patents), specify why and how long this will apply, bearing in mind that research data should be made available as soon as possible.

WP7/8: N/A

2.2. Making data accessible - Data:
Will the data be accessible through a free and standardized access protocol?

WP7: Yes, this will be provided by CORDIS.
WP8: No.

2.2. Making data accessible - Data:
If there are restrictions on use, how will access be provided to the data, both during and after the end of the project?

WP7/WP8: During the project, data will be stored in the project's repository: Sharepoint. The access to AGILE's Sharepoint is secured by 2 factor authentication, only invited members can access the project's sharepoint. If needed, personal data will be stored in folders with additionally restricted access.

2.2. Making data accessible - Data:

How will the identity of the person accessing the data be ascertained?

WP7/WP8: It will done by 2 factor authentication of Sharepoint.

2.2. Making data accessible - Data:

Is there a need for a data access committee (e.g. to evaluate/approve access requests to personal/sensitive data)?

WP7/WP8: For now there is not need for that.

2.2. Making data accessible - Metadata:

Will metadata be made openly available and licenced under a public domain dedication CC0, as per the Grant Agreement? If not, please clarify why. Will metadata contain information to enable the user to access the data?

WP7/WP8: N/A

2.2. Making data accessible - Metadata:

How long will the data remain available and findable? Will metadata be guaranteed to remain available after data is no longer available?

N/A

2.2. Making data accessible - Metadata:
Will documentation or reference about any software be needed to access or read the data be included? Will it be possible to include the relevant software (e.g. in open source code)?

WP7/WP8: No

2.3. Making data interoperable:
What data and metadata vocabularies, standards, formats or methodologies will you follow to make your data interoperable to allow data exchange and re-use within and across disciplines? Will you follow community-endorsed interoperability best practices? Which ones?

WP7/WP8: n/a

2.3. Making data interoperable:

In case it is unavoidable that you use uncommon or generate project specific ontologies or vocabularies, will you provide mappings to more commonly used ontologies? Will you openly publish the generated ontologies or vocabularies to allow reusing, refining or extending them?

WP7/WP8: N/A

2.3. Making data interoperable:
Will your data include qualified references[1] to other data (e.g. other data from your project, or datasets from previous research)?

[1]*A qualified reference is a cross-reference that explains its intent. For example, X is regulator of Y is a much more qualified reference than X is associated with Y, or X see also Y. The goal therefore is to create as many meaningful links as possible between (meta)data resources to enrich the contextual knowledge about the data. (Source:* https://www.go-fair.org/fair-principles/i3-metadata-include-qualified-references-metadata/***)***

unlikely

2.4. Increase data re-use:
How will you provide documentation needed to validate data analysis and facilitate data re-use (e.g. readme files with information on methodology, codebooks, data cleaning, analyses, variable definitions, units of measurement, etc.)?

WP7: N/A
WP8: N/A

2.4. Increase data re-use:
Will your data be made freely available in the public domain to permit the widest re-use possible? Will your data be licensed using standard reuse licenses, in line with the obligations set out in the Grant Agreement?

WP7: The deliverables will be made public, no other data output expected.
WP8: The deliverable D8.1 and related documents are considered "sensitive", not public.

2.4. Increase data re-use:
Will the data produced in the project be useable by third parties, in particular after the end of the project?

WP7: deliverables such as Project Management Guide, Risk Management Plan, Data Management Plan can be used for reference and consideration for future Horizon project beneficiaries/coordinators
WP8: deliverable and related documents are considered "sensitive", not public

2.4. Increase data re-use:

Will the provenance of the data be thoroughly documented using the appropriate standards?

WP7/WP8: Yes, if required, but it is unlikely that is is applicable.

2.4. Increase data re-use:

Describe all relevant data quality assurance processes.

We will rely on the best practices on the domain and call on the data support team at Johanniter Unfall Hilfe and Arttic.

2.4. Increase data re-use:

Further to the FAIR principles, DMPs should also address research outputs other than data, and should carefully consider aspects related to the allocation of resources, data security and ethical aspects.

No data concerns are expected for WP7 and WP8.

Other research outputs

In addition to the management of data, beneficiaries should also consider and plan for the management of other research outputs that may be generated or re-used throughout their projects. Such outputs can be either digital (e.g. software, workflows, protocols, models, etc.) or physical (e.g. new materials, antibodies, reagents, samples, etc.).

n/a

Beneficiaries should consider which of the questions pertaining to FAIR data above, can apply to the management of other research outputs, and should strive to provide sufficient detail on how their research outputs will be managed and shared, or made available for re-use, in line with the FAIR principles.

n/a

Allocation of resources

What will the costs be for making data or other research outputs FAIR in your project (e.g. direct and indirect costs related to storage, archiving, re-use, security, etc.) ?

storage on Sharepoint provided through ARTTIC - costs related to the project unknown, please see WP6; publication of project results on CORDIS without costs

How will these be covered? Note that costs related to research data/output management are eligible as part of the Horizon Europe grant (if compliant with the Grant Agreement conditions)

n/a

Who will be responsible for data management in your project?

WP7: project coordinator (JUH) and project office (ARTTIC)

WP8: Project coordinator (JUH)

How will long term preservation be ensured? Discuss the necessary resources to accomplish this (costs and potential value, who decides and how, what data will be kept and for how long)?

WP7: data will be kept for the duration stated in the Grant Agreement, either in project's sharepoint and/or locally at Johanniter
WP8: data will be kept for the duration stated in the Grant Agreement, either in project's sharepoint and/or locally at Johanniter

Data security

What provisions are or will be in place for data security (including data recovery as well as secure storage/archiving and transfer of sensitive data)?

WP7: Sharepoint repository is only accessible with 2 Factor Authentication, laptops/computers/mobile devices are secured by password; oldes versions of a document can be recovered through Sharepoint's version control; deleted documents can be restored from the trash folder within Sharepoint

WP8: Sharepoint repository is only accessible with 2 Factor Authentication, laptops/computers/mobile devices are secured by password; oldes versions of a document can be recovered through Sharepoint's version control; deleted documents can be restored from the trash folder within Sharepoint

Ethics

Are there, or could there be, any ethics or legal issues that can have an impact on data sharing? These can also be discussed in the context of the ethics review. If relevant, include references to ethics deliverables and ethics chapter in the Description of the Action (DoA).

WP8: D8.1 has defined a process on how to handle ethics issues. AGILE's approach to deal with relevant topics from the ethics self-assessment (AI, personal data, non-EU participants, human participants) will be addressed in additional internal guidelines, as explained in D8.1

Will informed consent for data sharing and long term preservation be included in questionnaires dealing with personal data?

WP7: yes
WP8: yes

Other issues

Do you, or will you, make use of other national/funder/sectorial/departmental procedures for data management? If yes, which ones (please list and briefly describe them)?

No.