Data Privacy Project

PROJECT PLAN

Huijser, D.C. (Dorien) & Moopen, N. (Neha)
RDM SUPPORT | UTRECHT UNIVERSITY

VERSION: 1.2, LAST EDITED: 2022-03-18

Contents

INTRODUCTION **3**

BACKGROUND 3
AIMS 3
TARGET AUDIENCE 4
UNIQUE VALUE PROPOSITION 4
RELATED DOCUMENTATION 4

DELIVERABLES **5**

DATA PRIVACY HANDBOOK 6
Workflow *6*
Post-Publication *7*
USE CASES 10
Strategy *10*
SURVEY & INTERVIEWS 9
DISSEMINATION 12

HOW DO WE MAKE IT WORK? **13**

ROLES AND RESPONSIBILITIES 13
Steering Group *13*
Project Coordinators *13*
Project Team *13*
Stakeholders *14*
Communication Plan *14*
LIFE AFTER THE DATA PRIVACY PROJECT 15
Afterlife of the project deliverables *15*
Afterlife of the working group *16*
STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS (SWOT) 17
Strengths *17*
Weaknesses *18*
Opportunities *19*
Threats *19*
POTENTIAL SOLUTIONS *19*

APPENDIX A. COMMUNICATION PLAN **21**

APPENDIX B. STAKEHOLDER ANALYSIS **23**

Introduction

BACKGROUND

Scientific research often includes some form of personal data. The amount of personal data in research is likely underestimated, as researchers may be unaware of what personal data are or whether they are being collected. With the implementation of the General Data Protection Regulation (GDPR) in May 2018, stricter legal requirements apply to handling personal data and its sharing or publication. The number of (complex) questions on handling personal data in scientific research is increasing. Yet, practical information to resolve these questions is difficult to find, scattered, and/or discipline-specific. As such, there is room to better translate the legislation to scientific research practice and to provide practical tools for handling personal data in research.

AIMS

The aim of this project is to build knowledge and expertise on how researchers can and should deal with personal data. Specifically, the project has four goals:

1. Create a knowledge base for researchers to learn about (research) data privacy, including GDPR-compliant best practices and privacy-enhancing techniques.

2. Develop or document existing tools that can be used to address concrete data privacy-related issues. A tool repository will be curated to complement the aforementioned knowledge base.

3. Perform qualitative and quantitative investigations into (current) practices and needs of researchers in handling personal data and complying with the GDPR.

4. Provide (a start for) training materials for researchers and support staff on handling personal data and using the available tools.

TARGET AUDIENCE

Researchers at Utrecht University (UU) are the primary target audience, while UU scientific support staff are the secondary target audience. The project output will be available publicly, so that external researchers and support staff may also access them, making them a tertiary target audience.

UNIQUE VALUE PROPOSITION

The project outputs will be Findable, Accessible, Interoperable, Reusable (FAIR) for the target audiences. Particularly, they will be practical and actionable so that target audiences can apply them in their own situation.

Moreover, we will be collaborating across several teams: data management (both library as well as faculty staff), privacy officers, research engineers, legal affairs, open science, and researchers to ensure the project output is based on combined expertise and consensus.

RELATED DOCUMENTATION

All project documentation can be found in the Data Privacy Project Teams environment, the project website, and the Data Privacy Handbook.

Deliverables

The following deliverables are planned in line with the (specific) project aims:

1. Data Privacy Handbook
2. Survey & Interviews
3. Use Cases
4. Dissemination

HANDBOOK

Created by Anconer Design from Noun Project

SURVEY

Created by Jaime Carrion from Noun Project

USE CASES

Created by Vectors Market from Noun Project

DISSEMINATION

Created by priyanka from Noun Project

DATA PRIVACY HANDBOOK

The Data Privacy Handbook is an open-source, community-driven Handbook about handling personal data in scientific research in line with the GDPR (see also the GitHub repository). It consists of:

- a knowledge base, covering topics like privacy by design, personal data sharing and legal documents to handle personal data;
- a tool repository, containing tools for, for example, pseudonymizing, encrypting or sharing personal data;
- use cases: research projects with typical privacy-related issues, for which a reusable solution (e.g., tool, workflow) has been developed.

As far as possible, the content of the Handbook will be practical and actionable, for example by providing workflows, tools and practical translations of the GDPR, without unnecessary detail and jargon.

Knowledge on privacy-related laws, tools, and strategies is scattered and differs in depth and usefulness across (UU) websites and teams (such as privacy, data management, research departments, faculties, etc.). With the Data Privacy Handbook, this information will be collaboratively synthesized into one resource, which readers can consult and (re)use.

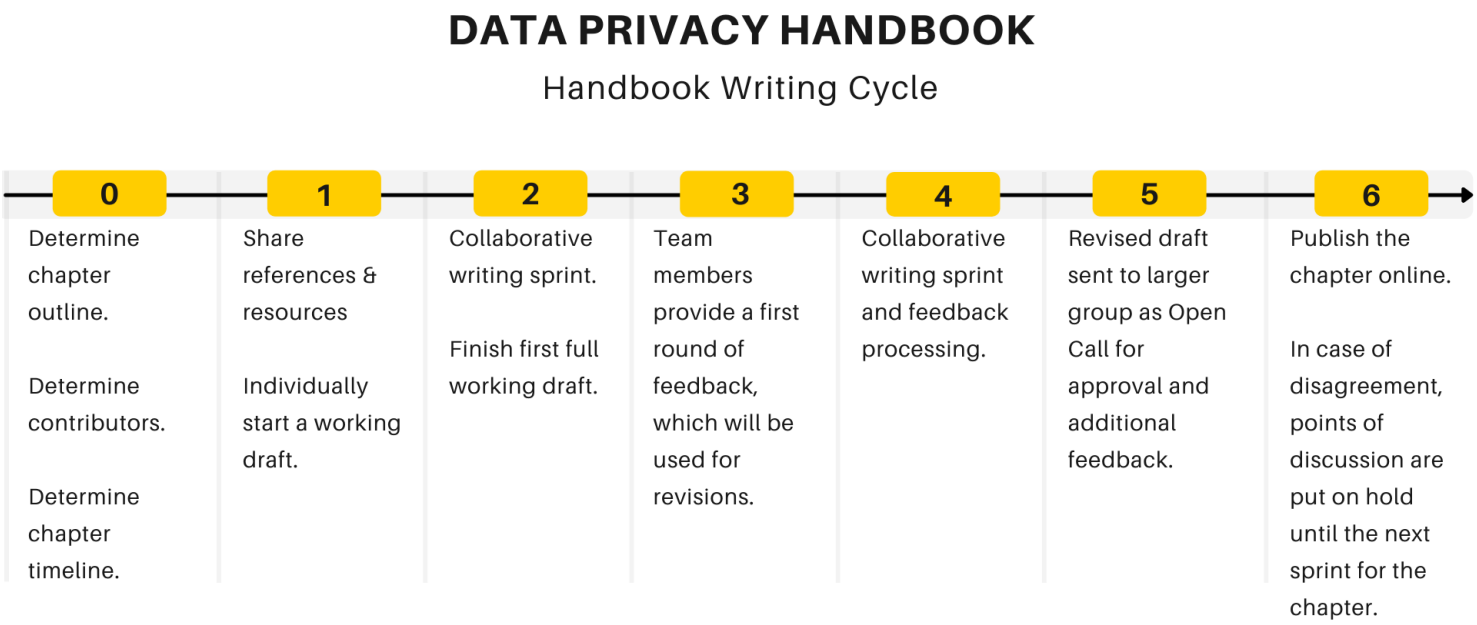
Workflow

For the initial writing of Handbook chapters, we will work in cycles, each consisting of collaborative book sprints to work on a single Handbook chapter and several feedback moments. This format was chosen, because it has proven difficult to plan the Handbook across longer time frames. The cycles will include concrete goals and deadlines, which will create clarity and increase accountability for everyone involved.

That being said, the way of working within the cycle and the contents developed are flexible: the focus is to reach a broad goal (e.g. complete a chapter), not to follow a detailed plan.

This format allows us to involve contributors more flexibly: anyone interested in the topic can join the book sprints,. Contributors can determine for themselves which chapters they are interested in working on, without compelling them to be involved in chapters less relevant to them.

Concretely, a book sprint may look like this:



Chapter Publication

To ensure that content in the Handbook is widely supported, we aim to get a 'green light' from as many relevant stakeholders as possible before publishing a chapter. Team members who are not involved in writing a specific Handbook chapter will nonetheless be invited to provide feedback. We will also send drafts to our wider network of stakeholders, including (first- and second-line) privacy officers., who are offered the opportunity to 'green-' or 'red-light' (parts of) the chapter.

If someone objects to (part of) a Handbook chapter, we will address their concerns to the best of our abilities and publish the chapter with our edits. If a majority of contributors and/or stakeholders object to the chapter, we will refrain from publishing the chapter and

return to it in a next cycle. If no agreements can be made, we will consult with the steering group to discuss further steps.

Post-Publication

When a chapter has gone through the two feedback phases, giving stakeholders the opportunity to give their feedback and/or 'red'-light, the content will be published and visible immediately on a webpage rendered with GitHub Pages. Since the Handbook will be publicly available, we will include disclaimers where possible, explaining the liabilities and terms of use.

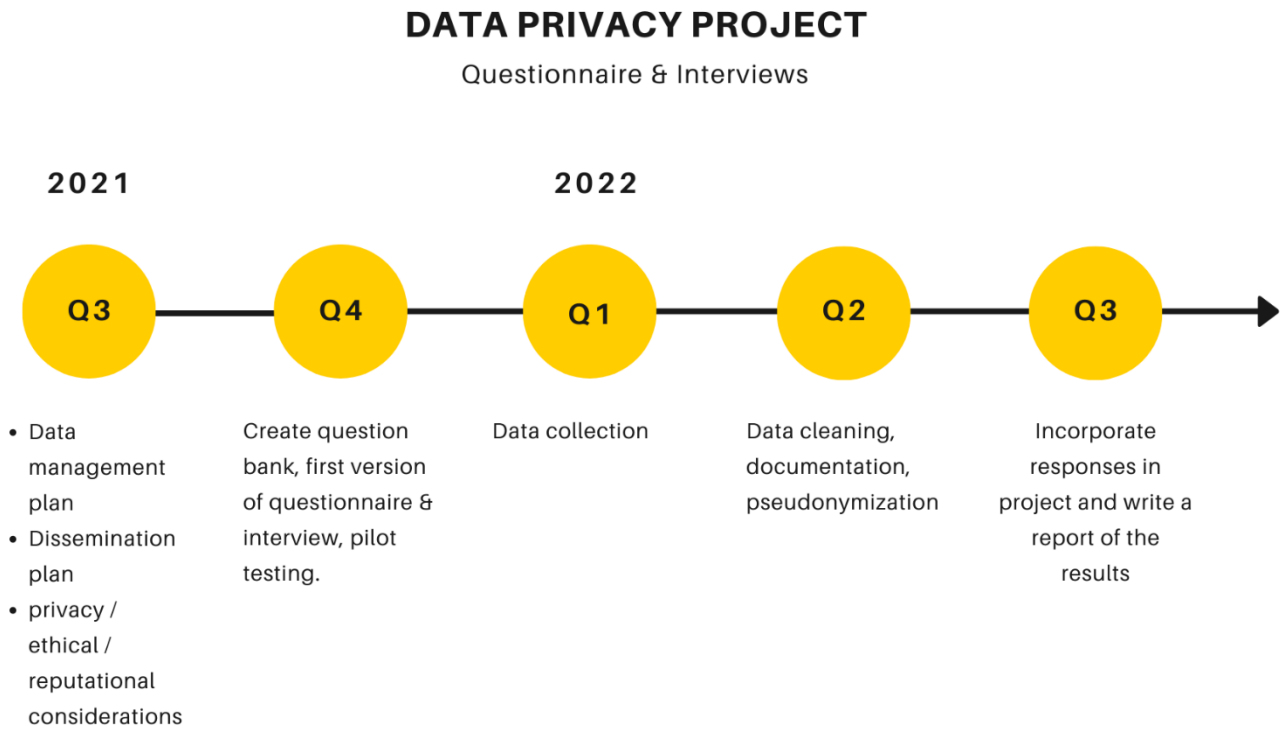
For individuals with a GitHub account, Contributing Guidelines are available if they would like to provide feedback on published chapters. For now, those without a GitHub account can provide feedback to the project coordinators via email. In the future, a more automated procedure through which non-GitHub users can provide feedback may be created.

SURVEY & INTERVIEWS

A university-wide survey will be conducted among researchers, who form our target audience. The survey is meant to develop insight into researchers' experiences in handling personal data. It will cover the privacy-related issues they run into, their current approach and practices, and their needs and requirements in terms of support.

The survey will include a questionnaire as well as interviews with researchers. This will provide both quantitative and qualitative input for reporting purposes, as well as an evidence-base to guide the project as it evolves.

The strategy and an estimated timeline for the survey is outlined below:



USE CASES

In order to develop tools and solutions that can be applied to various research projects, we will take on use cases. Use cases are privacy-related questions/issues experienced within research projects and the implemented or proposed solutions to those issues (which may be developed during this project). They may concern challenges in safely collecting, analyzing, storing, or sharing privacy-sensitive research data. Possible solutions can range from workflows for de-identification or data sharing, contractual templates (informed consent, data transfer or processing agreement, etc.), to (research) software solutions.

By taking on use cases, the project will actively support researchers with ongoing challenges in handling personal data and simultaneously develop solutions that can be reused by other researchers and support staff in the future.

Strategy

A call for use cases was put out in September 2021. Additionally, incoming questions and projects to the involved stakeholders (e.g., RDM Support, Research Engineering, privacy officers, data stewards) may be assessed for their suitability. Moreover, ongoing projects at RDM Support or Research Engineering that meet the use case criteria can receive additional support – particularly in FAIRification.

Use cases will be worked on in parallel and team members may join freely or by invitation depending on their expertise and availability. The specific steps in tackling a use case will likely vary across projects. In due course, the solutions will be FAIRified and described in the Data Privacy Handbook.

The criteria for incorporating a use case can be found in the call for use cases.:

- The research project includes personal data in any type or form.

- A solution for de-identifying or safely handling personal data is required (or has been implemented already), for example pseudonymization, federated analysis, synthetic data, workflows, templates, etc.
- The potential solution can be FAIRified and reused by other researchers.
- The researcher(s) is/are prepared to work closely with the project team on the solution.

DISSEMINATION

As the project output becomes more defined, we will incorporate it into new and existing dissemination materials to educate the target audiences and create awareness of the subject.

Opportunities for dissemination may include:

- Workshops & courses on (research) data privacy. These may be online or offline, for self-study or otherwise. Content developed during the project may be used to complement existing training materials and information (e.g., RDM Support's course on "Handling Personal Data" and faculty-specific websites) or to create a broader curriculum (e.g., a self-study module on the Life Long Learning platform).
- Presentations for researchers at the project, department, faculty-levels, from PhD candidates to Principle Investigators.
- Presentations for research communities, e.g., the Open Science Community Utrecht (OSCU).
- Presentations for UU and (inter)national data management communities.
- A network of Privacy Champions within faculties, similar to the OSCU Ambassadors or Faculty Open Science Track (FOST) representatives.

How do we make it work?

ROLES AND RESPONSIBILITIES

Steering Group

The steering group meets with the project coordinators, will keep an eye on the project's progress and will provide additional help where necessary. The steering group for this project consists of:

- Kim Bergmans, Department Manager, Academic Services, University Library.
- Frank Heere, Department Manager, Information & Technology Services (ITS).
- Kees Zandbergen, Department Manager, Collection Services, University Library (August-December 2021).

Project Coordinators

The project coordinators are data managers who function as the main point of contact for the project. They organize meetings and communicate with stakeholders, monitor project progress, and work on all deliverables of the project themselves. They are:

- Neha Moopen, Research Data Manager, University Library (0.4 fte).
- Dorien Huijser, Research Data Manager, University Library (0.6 fte).

Project Team

The project team works actively on the project together with the project coordinators / data managers. Members volunteer their time and therefore, contributions and time investments may differ. New team members may join anytime and existing team members may leave over time. At the moment, the project team consists of:

- Francisco Romero Pastrana, Privacy Officer, Faculty of Geosciences.
- Jacques Flores, Data Consultant, University Library.

- Saskia van den Hout, Information Security Officer, ITS.
- Danny de Koning-van Nieuwamerongen, Data Manager, University Library.
- Ron Scholten, Data Manager, University Library.
- Robert Steeman, Privacy Officer, Faculty of Social and Behavioral Sciences.
- Frans Huigen, Privacy Officer, Faculty of Science.
- Martine de Vos, Coordinator Research Engineering, ITS.
- Garrett Speed, Data Steward, Faculty of Geosciences.
- Johanneke Siljee, Second-line Privacy Officer, Legal Affairs.
- Raoul Schram, Research Engineer, ITS.
- Frans de Liagre Böhl, Data manager, Faculty of Humanities.

Alumni:

- Menno Rasch, Initiator and previously project manager of this project, ITS.
- Annemiek van der Kuil, Previously Coordinator Research Data Management Support, University Library.
- Liliana Vargas Meleza, Previously Data Steward, Faculty of Geosciences.
- Sanne Kleerebezem, Previously Privacy Officer, University Library & Faculty of Veterinary Sciences.

Communication Plan

A detailed Communication Plan has been drawn up to ensure all stakeholders are kept informed on and involved in developments in the project.

Stakeholders

There are numerous stakeholders in this project, including the Privacy Officers & Research Engineers. For an overview of all stakeholders and their involvement, please refer to the Stakeholder Analysis (see Appendix B).

LIFE AFTER THE DATA PRIVACY PROJECT

The Data Privacy Project has funding until July 2023. This section addresses activities and sustainability of the deliverables after the project's end date.

Afterlife of the project deliverables

Data Privacy Handbook

The Data Privacy Handbook will keep on existing in two forms:

- The Handbook will be archived on Zenodo. This will ensure that a snapshot of the Handbook will be retained, creating a digital object that can be found via Zenodo's metadata and cited through the DOI.
- The website of the Handbook will stay live, so that it can continue to be consulted and possibly updated. The latter requires the GitHub repository to keep being maintained. For the coming years, RDM Support may be best suited to take this upon themselves.

Use Cases

The Use Cases we have worked on during the project and the solutions created will be documented in the Data Privacy Handbook. Where necessary, developed or curated tools will be FAIRified, aiding discovery and adoption by researchers and support staff.

Survey & Interviews

The Survey and Interviews will be finished by the end of the project. Its results will be made publicly available via a summary report and taken into account during the project itself.

Dissemination

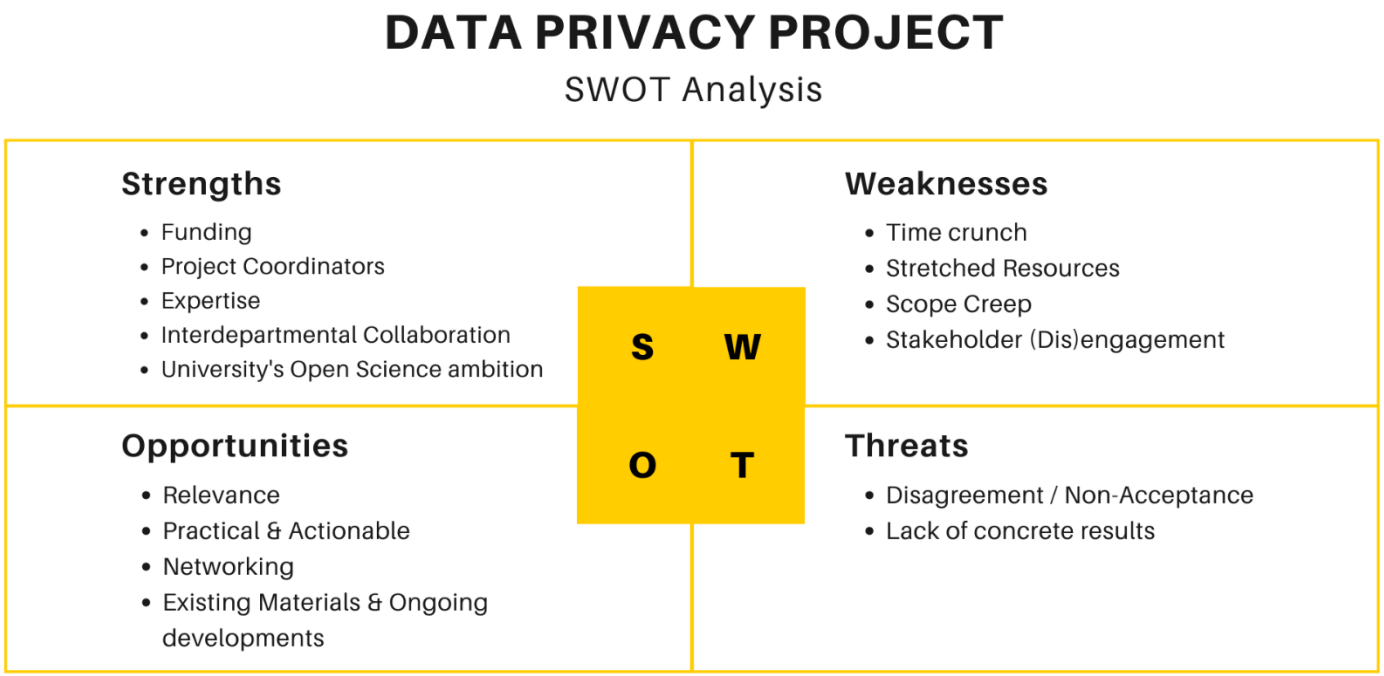
Dissemination will be the primary way of embedding the project's results into the organization. By providing (input for) trainings, workshops, presentations, etc., the output from this project can be implemented into scientific practice.

Afterlife of the working group

This project has effectively created a working group of data privacy experts within Utrecht University, who have greatly benefited from collaborating with each other. We hope to sustain this collaboration and implement it more structurally into the organization after the project has ended. A community manager at RDM Support may be able to assist with forming new avenues or channels for continued interaction and collaboration.

STRENGTHS, WEAKNESSES, OPPORTUNITIES, AND THREATS (SWOT)

For a strategic perspective on the project, an overview of the project's Strengths, Weaknesses, Opportunities, and Threats (SWOT) is presented below.



Strengths

These are internal factors that set the project up for success.

- Funding: The project has funding through the UU Research IT program and the NWO-DCC funding instrument. It provides for a (full-time) data manager and research engineer to work on the project until July 2023.
- Project Coordinators: Two data managers serve as 'coordinators' for the project, in addition to working on the deliverables. They maintain an overview of the project from its strategic standpoint to the day-to-day activities.

- Expertise: There is no dearth of expertise in the project team, which consists of specialists in the fields of data management, privacy, research software, information security, and open science.
- Interdepartmental Collaboration: The project involves significant collaboration between departments, which is advantageous compared to these departments working in 'silos'. The project team effectively functions an active working group on the topic.
- Utrecht University's ambitions and obligations: Utrecht University has ambitions to be at the forefront of open science whilst meeting its legal obligations under the GDPR. The organization is therefore driven to determine how personal data can be effectively (re)used in line with the GDPR.

Weaknesses

These are internal factors that (could) make it difficult for the project to succeed.

- Time Crunch: Some deliverables, such as the Handbook, are planned with (relatively) strict schedules. However, delays may be unavoidable considering the number of stakeholders. Timelines can therefore become tighter.
- Stretched Resources: All team members and stakeholders, apart from the project coordinators and involved research engineers, will be contributing on a voluntary basis. There is a risk of contributors realizing they are unable to contribute, due to limited time and capacity.
- Scope Creep: Given the breadth of the project, uncontrolled growth of the project's scope is a possibility – to the point where deliverables cannot be effectively managed by the project coordinators and team. Concretely, we may take up too many use cases, take too long finalizing a Handbook chapter, have too many people involved, or add another deliverable to the project.
- Stakeholder (Dis)engagement: Considering the number and range of stakeholders, disengagement – for example, due to misalignment of expectations and goals - should be prevented as it would reduce productivity.

Opportunities

Opportunities are the external factors that are likely to contribute to the project's success.

- Relevance: There is greater awareness of data privacy issues and more questions on the topic arise every year. This project fulfills a need from researchers and support staff.
- Practical & Actionable: There is a need for more hands-on resources on data privacy, the project output is intended to be easily picked up and implemented by researchers.
- Networking: Through collaboration, the network of data & privacy professionals and researchers can be further strengthened.
- Existing Materials & Ongoing Developments: Output from completed and current RDM/IT/privacy initiatives and policies already provide a basis for the project.

Threats

These are external factors that, if they were to occur, could harm the project.

- Disagreement / Non-Acceptance: Widespread support and consensus will be necessary for the project to succeed. Stakeholders' disagreement or non-acceptance of the deliverables would hinder progress and prevent dissemination of the output.
- Lack of Concrete Results: Given the range of stakeholders and expertise, (extended) abstract discussions, aimed at integrating different perspectives, could inadvertently prevent achieving concrete goals and results.

POTENTIAL SOLUTIONS

- Stretched Resources:
    - Make contributions explicit and concrete: giving specific assignments, setting deadlines and booking agenda time are all ways to establish this.
    - Connect with stakeholders' existing work to avoid double work.

- Scope Creep:
    - Determine clear boundaries, e.g., a minimal viable product, a maximum amount of use cases, etc.
    - Get support for project management and communication.
    - Set quarterly goals and evaluate how they contribute to the main project aims.
    - Ask important stakeholders for feedback on the project planning.

- Stakeholder (Dis)engagement:
    - Communicate clearly about the project, by having monthly team meetings, monthly email updates and sticking to one communication channel.
    - Work on tasks (e.g., the Handbook) together instead of individually. This will increase feelings of active involvement and wide-spread support and forces team members who are joining to spend time on the project.

- Disagreement / Non-Acceptance:
    - Involve privacy officers and faculty data support early on, by having them contribute actively to the project (thus becoming a project team member) and by including them in regular updates of the project.
    - Present the project at several occasions, e.g., to library staff, at faculties, external data support meetings, etc. to gain notoriety.
    - Meet with the Data Protection Office to get their acceptance of the project and the deliverables.

- Lack of concrete results:
    - Use explicit planning and communication to force to deliver a result.
    - Put the point of discussion on a backlog to go back to at a later time.
    - List several solutions if there is no agreement on a single one.
    - Use voting to make a decision.
    - Consult other relevant experts who may have a deciding voice.

Appendix A. Communication Plan

This communication plan concerns mainly communication about the status of the project. For the communication of the project output and results towards the target audience, we will have a dedicated dissemination plan.

WHAT	WHY	HOW	FREQUENCY	AUDIENCE	OWNER
WRITTEN COMMUNICATION					
Project update	Update the main stakeholders about the status of the project	Email	Monthly	Core team, Steering group, Interested stakeholders	Coordinators
News post	Comprehensive news update that is public and shareable as well.	Project website	Quarterly	Public	Coordinators
MEETINGS					
Steering Group meeting	Update about project and get input on how to proceed	Scheduled meeting	Quarterly	Steering group	Coordinators
Core team meeting	Discuss project progress and task division	Scheduled meeting	Monthly	Core team	Coordinators
Meeting with privacy officers	Awareness about project and get input on content	Scheduled meeting	1-2 times	First and second-line privacy Officers	Coordinators
Meeting with security officers	Awareness about project and get input on content	Scheduled meeting	1-2 times	Security Officers	Saskia
Research Engineering	Update about project and get practical input and strategy how to involve RE	Scheduled meeting	Monthly	Research Engineering, Martine de Vos	Coordinators
Verbal/semi-formal updates	Update about the project and get input on connecting	D-lunch	When necessary	RDM Support	Coordinators

Combined meeting	Update about the project and input	Scheduled meeting	Biannually	Privacy officers, security officers, research engineering	Coordinators
PRESENTATIONS					
Presentation	Update, feedback, networking	AS meeting	1-3 times	Library staff	Coordinators
		OSCU event		OSCU	
		Scheduled meeting		Faculty Open Science Teams, FAIR data and software fellows	
Presentation	Update, feedback, networking	Scheduled meeting	Biannually/Quarterly	Faculty liaisons	Coordinators
Presentation	Update, feedback, networking	RDM Expert meeting or UDMC	Biannually	RDM Support outside the library	Coordinators
ONLINE NETWORKING					
- Summary of and link to the quarterly news post - Call for proposals - Call for survey responses	Spread the word about the project and its progress and to get input on the project	Twitter: RDM support and personal accounts	Quarterly + additional calls when necessary	Twitter followers	Coordinators
		Slack: OSCU and DTL-DSIG		OSCU and DTL-DSIG	Coordinators
		GitHub Discussions		Public	Coordinators
		Intranet and OSCU website		Interested UU employees and researchers	Coordinators
		Mailing lists: RDM newsletters, faculty newsletters, etc.		Interested UU employees and researchers	Communication Coordinators
		RDM website		Interested UU researchers	Communication Coordinators
Project summary	Spread the word about the project and ask for input	Data management mailing lists (LCRDM, JISC)	Only when relevant	Interested external support staff	Coordinators

Appendix B. Stakeholder Analysis

A stakeholder is a person or an organization that is actively involved in the project or is positively or negatively impacted by it. A key stakeholder is any person who determines the success or failure of the project:

- Decision: Make the decisions that control or influence the project budget.
- Authority: Have the authority to grant permission to proceed with the project.
- Need: Directly benefit from or are impacted by the project and consequently need to know all about it.
- Connections: Are connected to the people, money, or resources required to remove roadblocks or exert influence to ensure project success.
- Energy: Have positive or negative energy that could affect project success.

STAKEHOLDER	ROLE IN PROJECT	KEY?	METHODS OF COMMUNICATION
Steering group	Decision, Authority, Connections, Energy	Yes	Regular Steering group meeting
RDM Support	Authority, Need, Connections, Energy	Yes	Regular Core team meeting
Research Engineering / Research & Data Management Services / ITS	Decision, Need, Connections, Energy	Yes	Regular meeting with Martine de Vos
Privacy Officers	Authority, Need, Connections, Energy	Yes	Meeting(s) with Privacy Officers
Information Security	Authority, Energy	Yes	Via Saskia Newsletter(s) and email
Legal Affairs	Authority, Energy	Yes	Meeting with Legal Affairs
Faculty Liaisons	Need, Connections, Energy	Yes	Presentation Newsletter(s) and email

Faculty Data Managers	Need, Connections, Energy	No	Presentation or one-on-one meetings Newsletter(s) and email
Ethical Committees	Energy	No	Newsletter(s) and email
Research Support Officers	Connections	No	Newsletter(s) and email
Communications department	Connections	No	Newsletter(s) and email
Academic Services	Connections, Energy	No	Academic Services meeting
Open Science Community Utrecht (OSCU)	Need, Connections, Energy	Yes	Newsletter(s) and email Slack Presentation
Faculty Open Science Teams (FOSTs)	Connections, Energy	No	Newsletter(s) and email Presentation
Open Science Fellows (FAIR data & software track)?	Need, Connections	No	Newsletter(s) and email Presentation
OSCU Ambassadors?	Need, Connections	No	Newsletter(s) and email Presentation
Researchers	Need, Connections, Energy	Yes	Presentation Newsletter(s) and email Connections (OSCU, privacy officers, data managers, etc.)
Graduate Schools	Need, Connections	No	Newsletter(s) and email
LCRDM	Need, Connections	No	Newsletter(s) and email
DTL-DSIG	Need, Connections	No	Newsletter(s) and email Slack
UKB	Need, Connections	No	Newsletter(s) and email
RDM Support & Privacy Officers at other universities	Need, Connections, Energy	No	Newsletter(s) and email Slack