

# Data Privacy Project

---

PROJECT PLAN

*July 2021 - June 2023*

# Contents

<b>INTRODUCTION</b>	<b>3</b>
BACKGROUND	3
AIMS	3
TARGET AUDIENCE	4
UNIQUE VALUE PROPOSITION	4
RELATED DOCUMENTATION	4
<b>DELIVERABLES</b>	<b>5</b>
DATA PRIVACY HANDBOOK	6
<i>Book Sprints</i>	6
<i>Workflow</i>	6
<i>Post-Publication</i>	7
USE CASES	8
<i>Criteria for Use Cases</i>	8
<i>Strategy</i>	8
SURVEY & INTERVIEWS	9
DISSEMINATION	10
<b>HOW DO WE MAKE IT WORK?</b>	<b>11</b>
ROLES AND RESPONSIBILITIES	11
<i>Steering Group</i>	11
<i>Project Coordinators</i>	11
<i>Project Team</i>	11
<i>Stakeholders</i>	12
<i>Communication Plan</i>	12
STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS (SWOT)	13
<i>Strengths</i>	13
<i>Weaknesses</i>	13
<i>Opportunities</i>	14
<i>Threats</i>	15
<b>APPENDIX A. COMMUNICATION PLAN</b>	<b>16</b>
<b>APPENDIX B. STAKEHOLDER ANALYSIS</b>	<b>19</b>

# Introduction

## BACKGROUND

Most scientific research contains some form of personal data. There is likely more such data than expected, with researchers being unaware of it. With the implementation of the General Data Protection Regulation (GDPR) in May 2018, stricter 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, 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.

## 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 **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. Build **training materials** and **courses/workshops** for researchers and support staff on handling personal data and using the available tools.

## TARGET AUDIENCE

Researchers (at Utrecht University) are the primary target audience, while scientific support staff (at Utrecht University) are the secondary target audience. The project output will be available to external researchers and support staff, thereby making them a tertiary target audience.

## UNIQUE VALUE PROPOSITION

The project output will be **Findable, Accessible, Interoperable, Reusable (FAIR)** for the target audiences. Particularly, it will be **practical** and **actionable** so that target audiences can apply it with ease.

Moreover, we will be collaborating across teams: data management, privacy, research engineering, legal affairs, open science, and everyone in between 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](#), the [Data Privacy Handbook](#) and the Project [Open Canvas](#).

# Deliverables

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

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

## DATA PRIVACY HANDBOOK

The [Data Privacy Handbook](#) is an open-source, community-driven, *living* Handbook (see also: [GitHub](#)) about handling personal data in scientific research, in line with the GDPR. It consists of a knowledge base, tool repository and use cases to draw inspiration from. As far as possible, the content of the Handbook will be practical and actionable, without unnecessary detail and jargon.

Knowledge on privacy-related laws, tools, and strategies is scattered and differs in depth and usefulness. With the Data Privacy Handbook, this information will be collaboratively synthesized into one resource, which users can consult at their convenience.

### Book Sprints

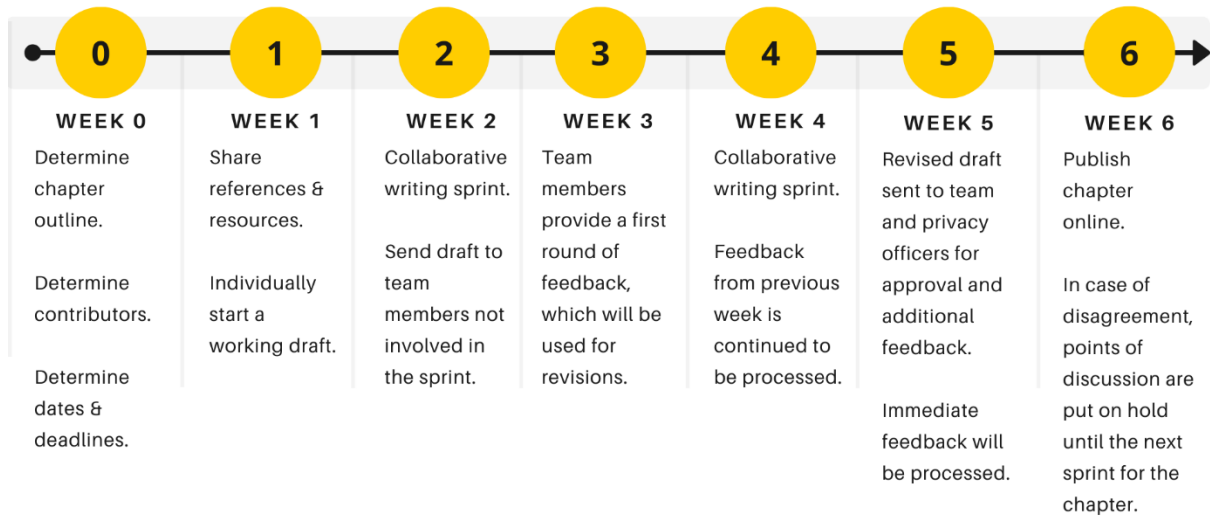
For the initial writing of Handbook chapters, book sprints following a **six-week cycle** will be carried out. This format was chosen, because it has proven difficult to plan this deliverable across longer time frames. The six-week cycles will include concrete goals and deadlines, which will create clarity and increase accountability for everyone involved. That being said, the way of working within the six weeks 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.

### Workflow

Every book sprint will emphasize a single Handbook chapter. This will be more focused than working on multiple chapters simultaneously. It will also prevent the trap of iterating a single chapter over months on end. Concretely, a book sprint may look like this:

## DATA PRIVACY HANDBOOK

Six-week cycle



### Post-Publication

When a chapter is approved and published via GitHub, the content will be visible immediately. 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 form through which non-GitHub users can provide feedback may be created, or functionality and tutorials to work on GitHub without an account (e.g., via HackMD) will be provided.

## **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 research projects that require support in tackling issues related to data privacy. They typically involve personal data in some form, and may have unclarities how to collect, analyze, store, or share the data. Possible solutions range from de-identification workflows and contractual templates to 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.

### **Criteria for Use Cases**

- The research project includes personal data.
- A solution for de-identifying or safely handling personal data is required, for example pseudonymization, federated analysis, synthetic data, workflows, templates, etc.
- The potential solution can be FAIRified and reused by other researchers.
- The use case can be tackled between now and January 2023.
- The involved researcher(s) is/are prepared to work collaborate with RDM Support.

### **Strategy**

A call for use cases will be put out in September 2021. Moreover, questions and projects that are sent to and handled by RDM Support, Research Engineering or stakeholders (e.g., privacy officers, data stewards) will be assessed for their suitability as use cases.

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 solution that is developed will be FAIRified and described in the Data Privacy Handbook.



## SURVEY & INTERVIEWS

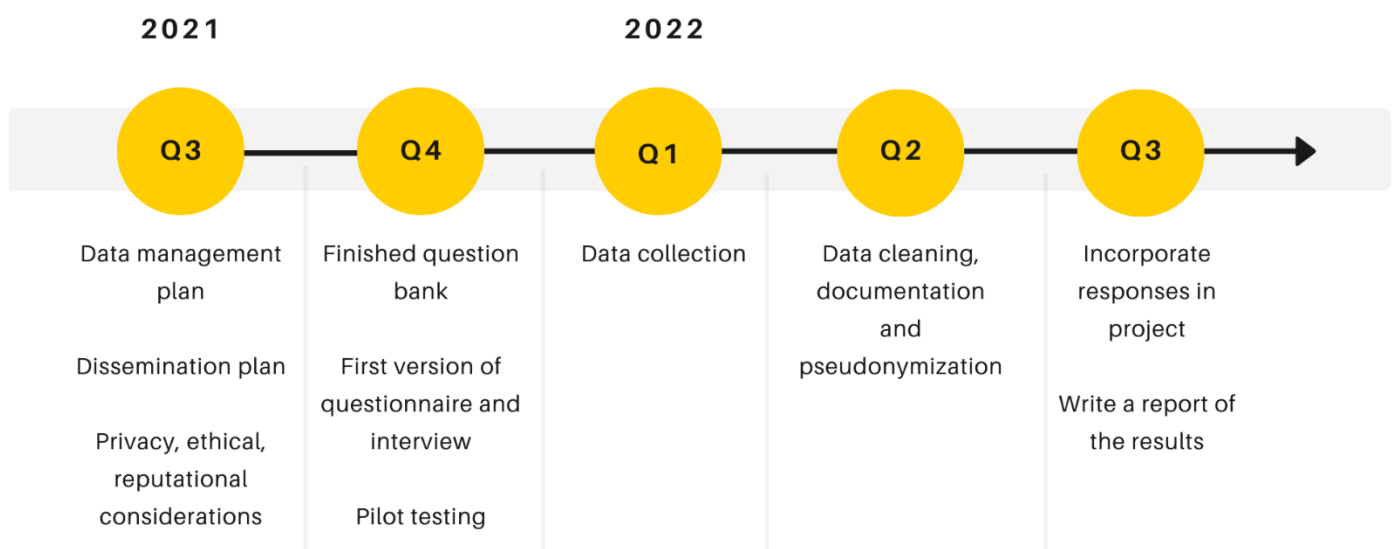
A university-wide survey will be conducted among researchers, who form our target audience. The survey is meant to develop insight into researchers' experiences in handling personal data. It will cover, but need not be limited to: the privacy-related issues they run into, their current approach and practices and their needs and requirements.

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:

### DATA PRIVACY SURVEY

#### Questionnaire & Interviews



## **DISSEMINATION**

As the project output becomes more defined, we will incorporate it into new and existing dissemination materials to educate the target audiences. Opportunities for dissemination may include:

- Workshops & courses on (research) data privacy. These may be online or offline, for self-study or otherwise.
- Presentations for researchers at the faculty, departmental and strategic theme-level.
- Presentations for researchers depending on their position: from PhD candidates to PIs.
- Presentations for research communities: for example, the Open Science Community Utrecht (OSCU).
- Presentations for UU and (inter)national data management communities.
- Setting up 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 and will place the project and its output at a strategic level in the institution. The steering group for this project consists of:

- **Kim Bergmans**, Department Manager, Academic Services, University Library
- **Frank Heere**, Department Manager, Information & Technology Services

### 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. The project coordinators are:

- **Neha Moopen**, Data Manager, University Library, 2 days/week
- **Dorien Huijser**, Data Manager, University Library, 3 days/week

### 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:

- **Sanne Kleerebezem**, Privacy Officer, University Library & Veterinary Sciences
- **Francisco Romero Pastrana**, Privacy Officer, Geosciences
- **Jacques Flores**, Data Consultant, University Library
- **Saskia van den Hout**, Information Security Officer

- Danny de Koning-van Nieuwamerongen, Data Manager, University Library
- Ron Scholten, Data Manager, University Library

## **Stakeholders**

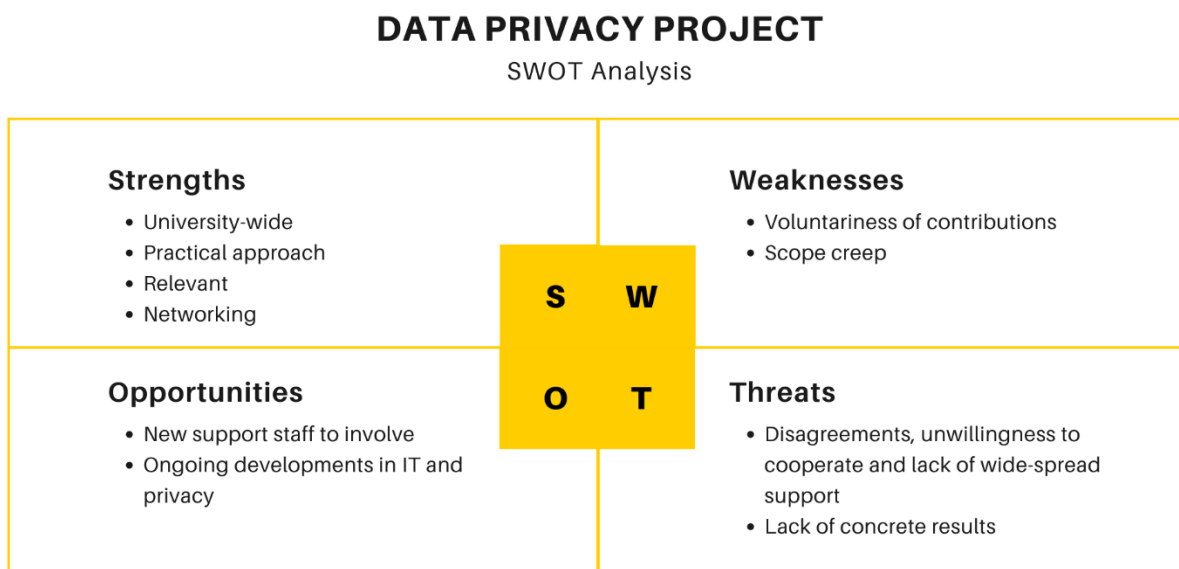
There are numerous stakeholders in this project, including the Privacy Officers & Research Engineers. For an overview of all stakeholders and their involvement, please refer to the Stakeholder Analysis ([see below](#)).

## **Communication Plan**

A detailed Communication Plan ([see below](#)) has been drawn up to ensure all stakeholders are kept informed on and involved in developments in the project.

## STRENGTHS, WEAKNESSES, OPPORTUNITIES AND THREATS (SWOT)

To determine how to tackle possible challenges, below we provide an overview of the project's Strengths, Weaknesses, Opportunities and Threats (SWOT). For the weaknesses and threats, we provide some ways of mitigating them.



### Strengths

- **University-wide approach:** we will give an opportunity to contribute to stakeholders across the university and beyond.
- **Practical approach:** the project's results will help researchers and support staff in practicing their job.
- **Relevant:** the project fulfills a need from both researchers and support staff.
- **Networking:** the project will create a network of privacy professionals across the university to be used and strengthened in the future.

### Weaknesses

- **Voluntariness of contributions:** stakeholders have to make time as they contribute on a voluntary basis. Therefore, it is a fine line between being too open-ended - creating low

accountability - and forcing team members to contribute if they are not able to - creating an unwillingness to contribute.

A few strategies we can use to mitigate this:

- 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.
  - 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.
- **Scope creep:** A great amount of stakeholders is involved, which makes it difficult to coordinate the project and to keep the scope of the project focused. For example, 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.

Some strategies we can use to mitigate this:

- 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.

## **Opportunities**

- **New support staff** is being hired throughout the university: they can contribute to the project while also learning about the university's support structure.

- There are many **ongoing developments** within IT and privacy that we can (re)use for the project.

## Threats

- Disagreement between stakeholders or unwillingness to cooperate may hinder the gaining of **wide-spread support** for the project. As this is a university-wide project, it may be a challenge to get everyone on the same page and implement our deliverables in practice. In particular, the privacy landscape is broad and knows many interpretations, which may cause disagreements. Moreover, we will have to deal with the fact that faculties or even institutes within them have policies and practices that vary widely.

A few things we can do to prevent this becoming a problem:

- 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 (see the [Communication plan](#)).
  - Meet with the Data Protection Office to get their acceptance of the project and the deliverables.
- Ongoing discussions and difficulties to integrate the legal, IT and data management components of the project may lead to endless discussions about specific details and as such a **lack of concrete results**.

We can:

- 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
<b>WRITTEN COMMUNICATION</b>					
Project update	Update the main stakeholders about the status of the project	Email	Monthly	Core team, Steering group, Interested stakeholders	Coordinators
News post	Comprehensive, structured and public news update that can be shared via the Networking channels	Project website	Quarterly	Public	Coordinators
<b>ONLINE NETWORKING</b>					
- 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	<b>Twitter:</b> RDM support and personal accounts	Quarterly + additional calls when necessary	Twitter followers	Coordinators
<i>idem</i>	<i>idem</i>	<b>Slack:</b> OSCU and DTL-DSIG	<i>idem</i>	OSCU and DTL-DSIG	Coordinators
<i>idem</i>	<i>idem</i>	<b>GitHub</b> Discussions	<i>idem</i>	Public	Coordinators
<i>idem</i>	<i>idem</i>	<b>Intranet</b> and OSCU website	<i>idem</i>	Interested UU employees and researchers	Coordinators



<i>idem</i>	<i>idem</i>	<b>Mailing</b> lists: RDM newsletters, faculty newsletters, etc.	<i>idem</i>	Interested UU employees and researchers	Communication Coordinators
<i>idem</i>	<i>idem</i>	RDM website	<i>idem</i>	Interested UU researchers	Communication Coordinators
Summary of project and link to project website	Spread the word about the project and ask for input	Data management mailing lists (LCRDM, JISC)	Only when relevant	Interested external support staff	Coordinators
<b>PRESENTATIONS</b>					
Presentation	Update, feedback	Academic services meeting	1-3 times	Library staff	Coordinators
Presentation	Update, feedback, networking	Scheduled meeting	Biannually/ Quarterly	Faculty liaisons	Coordinators
Presentation	Update, feedback	Scheduled meeting	Quarterly	Privacy officers	Coordinators
Presentation	Update, feedback	Open Science Community Utrecht	1-3 times	Researchers and support staff from OSCU	Coordinators
Presentation	Update, networking	Scheduled meeting	1-3 times	Faculty Open Science Teams	Coordinators
Presentation	Update, networking	Scheduled meeting	1-3 times	FAIR data and software fellows	Coordinators
Presentation	Update, feedback, networking	Scheduled meeting	Biannually	Research engineers	Coordinators
Presentation	Update, feedback, networking	RDM Expert meeting or UDMC	Biannually	RDM support outside the library	Coordinators
<b>MEETINGS</b>					
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	Update about project and get input on content	Scheduled meeting	Quarterly	Privacy officers	Coordinators
Meeting with security officers	Update about project and get input on content	Scheduled meeting	Biannually	Security officers	Saskia

Research engineering meeting	Update about project and get practical input and strategy how to involve RE	Scheduled meeting	Monthly	Research engineering, Martine de Vos	Coordinators
Coworking / Open Meeting	Work together on progressing the project	Scheduled afternoon meeting	1-2 times	Public	Coordinators
Verbal updates	Update about the project and get input on connecting	D-lunch	Monthly, when necessary	RDM support	Coordinators
Legal affairs meeting	Update about the project and input	Scheduled meeting	Biannually	Legal affairs	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