# Data Privacy Survey

Recommendations for improving privacy-related services for research at Utrecht University

Dorien Huijser*, Neha Moopen†& Rik D.T. Janssen‡

2022-10-26

**Abstract**

In the second quarter of 2022, Utrecht University (UU) Research Data Management Support (RDM Support) sent out a survey among all scientific personnel at UU, and organised one-on-one meetings with a selection of them. The aim of these efforts was to investigate 1) How UU researchers currently deal with personal data in their research, 2) What challenges they run into when handling personal data in research, and 3) How support at UU can improve their services concerning personal data in research. The results showed that most researchers knew to take privacy into account in their projects. However, there were vast differences in knowledge on this topic, as well as in how privacy-related practices were applied. Many researchers expressed concerns on the current quantity, findability and quality of privacy-related support at UU. These concerns were translated to recommendations in the current report. In short, our recommendations concern organising privacy-related research support in a way that makes handling personal data less of a burden for researchers. Moreover, it is important to increase the visibility and findability of existing and new privacy-related support, and create materials and expertise that are more tailored to academic practice. Taking up these recommendations within the organisation will likely both increase overall GDPR compliance and help researchers focus more on performing high-quality research.

## Contents



*Research Data Management Support, Utrecht University, ORCID: 0000-0003-3282-8083

†Research Data Management Support, Utrecht University, ORCID: 0000-0003-1412-4402

‡Information Technology Services, Utrecht University, ORCID: 0000-0001-9510-0802

# 1 Introduction

Scientific research often includes some form of personal data. However, 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 2018, stricter legal requirements apply to handling personal data and its sharing and publication. In our own experience, the number and complexity of questions on handling personal data in scientific research at Utrecht University (UU) is increasing.

Our goal at Research Data Management Support (RDM Support) is to assist researchers with any issues surrounding the management of their research data, including research data that contain personal data. To understand how we can best help researchers with their privacy-related questions and needs, we wanted to investigate:

1. To what extent are UU researchers aware of privacy legislation and practices?
2. What data privacy issues do UU researchers typically run into?
3. What support do UU researchers need to handle personal data?

To answer these questions, we set up an online survey and planned one-on-one meetings with a selection of UU researchers. This report summarises our findings, and describes recommendations to improve privacy-related services for research at Utrecht University. For a full description of the methods and results, please refer to the Data Privacy Survey Report.

This survey was part of a larger project, the Data Privacy Project[1], a data support effort led by RDM Support at UU that aims to provide actionable and FAIR (Findable, Accessible, Interoperable, Reusable) information and tools for researchers to handle personal data in their research.

# 2 Methods summary

The Data Privacy Survey consisted of two parts:

- An online survey that was sent to all of UU's scientific personnel via email, asking about researchers' current practices in handling personal data in their research, awareness of data support channels, and challenges and needs in this area.
- One-on-one meetings with individual researchers to talk about their experiences, challenges and needs in this area.

All relevant materials can be found in the GitHub repository and are described in the full report.

# 3 Results summary

Below is a summary of all results, which are described in full in the Data Privacy Survey Report.

## 3.1 Current practices

The Data Privacy Survey showed that personal data are processed in research from each faculty and across all academic positions at Utrecht University. Most researchers indicated to be familiar with concepts like anonymisation and pseudonymisation, access control, and UU-approved tools for handling personal data.

[1]The Data Privacy Project was funded by Utrecht University's Research IT program and a Digital Competence Center grant from the Dutch Organization for Scientific Research (NWO).

However, the knowledge level differed quite a bit. For example, some researchers indicated storing personal data on locations where it is officially not allowed. Data sharing was common, but the right measures were not always taken to do so securely. Additionally, some measures to securely handle personal data in accordance with the GDPR seemed to be unknown, such as the processing register, Data Protection Impact Assessment, and Standard Contractual Clauses. Finally, there seemed to be a lack of clarity among researchers on specific issues, such as when sharing data is allowed, or when data are personal.

### 3.2 Challenges and needs

In both the survey and the one-on-one meetings, many researchers mentioned that privacy caused a high administrative burden in the research process. For example, they mentioned that processes have taken a long time to complete (e.g., writing and reviewing a Data Privacy Impact Assessment), and that there are too many forms to be filled out which have overlapping content. Examples of such forms are the Data Management Plan, Privacy scan, Data Protection Impact Assessment, and the ethics application in which privacy is sometimes also included.

The high administrative burden was also partly caused by the fact that researchers did not know what was expected of them: what actions are required from their side, when and from whom should they ask help? The latter question is relevant when considering the large variety of support personnel in each faculty: privacy officers, data managers, security officers, Ethical Review Boards, Research Support Officers and the Data Protection Officer can all help researchers, but their exact role is often unclear to researchers and may even differ across faculties.

Some researchers were not content with the support they had received in the past. For example, their research project may have suffered significant delays due to the fact that support personnel only pointed them at what they could not do, rather than how to solve privacy-related issues. We noticed many researchers that argued for more hands-on support, rather than advise with no concrete direction on how to apply it in practice.

Several researchers noted that they found it difficult to find the correct (UU-specific) information and tools to handle personal data in research, in some cases leading to them "googling" for the information they needed. This was due to two reasons:

- A large amount of places that contain such information: the intranet pages on Privacy and Research, the RDM Support website, websites from the Ethical Review Boards, faculty data support websites, etc. Researchers indicated to find it hard to assess which information resource was the one they should be using.
- Existing information was too abstract, contained too much jargon to understand, was not tailored to research, or not tailored to specific research scenarios.

Finally, many problems seemed to arise from the fact that privacy had not been taken into account from the design phase of a research project. This generally led to data support staff being contacted too late in the process, who then had to tell the researcher to retrospectively make changes in their design in order to move forward.

## 4 Recommendations

Based on our findings, the most important recommendation we want to highlight is to decrease the burden on researchers to protect personal data throughout the research cycle. As described above, many researchers see privacy as an administrative hurdle, which takes up too much of their time and effort. Below we make this recommendation more concrete:

- Provide clarity on the process and responsibilities of researchers and data support staff

- Smoothen the process of handling personal data in research
- Make current and future information and tools better findable
- Increase the hands-on nature of support
- Improve the quality of information and tools

## 4.1 Provide clarity on the process and responsibilities of researchers and data support staff

We recommend to create a clear overview of labour and responsibility of both researchers and all types of data support staff. Which steps do researchers have to take before they can start executing their research, who is responsible for (supporting) which step, and when is there an official "green light" for researchers to move forward with their project?

Faculty-level support, consisting of privacy officers, data managers, Research Support Offices, and Ethical Review Boards, should come to agreements on support routing: which steps should researchers take when processing personal data, which support staff team tackles which kind of questions, and when should researchers contact them? A good example has been set by the Faculty of Geosciences, in which all faculty-level data support is organised in one team, the members of which regularly discuss cases and prevent projects from falling through the cracks or contacting a privacy expert too late in the process.

## 4.2 Smoothen the process of handing personal data in research

As indicated by many researchers, the administrative burden of preparing research can be greatly reduced if the overlap between several forms is decreased. Our recommendation is therefore to use one system for all research-related administration. Such a system should include not only the Data Management Plan, but also the ethical application (if applicable), Privacy scan, Data Protection Impact Assessment, and processing register. A similar infrastructure is currently being built at the Faculty of Humanities and may be valuable to also use at all other faculties.

Additionally, to lower the administrative burden, the process of performing a Data Protection Impact Assessment (DPIA) should be smoother and more clear: privacy officers should make agreements on when a DPIA should be performed. DPIAs from similar projects – also from other faculties if relevant - should be reused to prevent having to perform a DPIA from scratch. Ideally, a DPIA should only be performed if absolutely necessary. At the moment, UU's privacy officers are already working on this recommendation.

## 4.3 Make current and future information and tools better findable

As several researchers indicated to have difficulties finding the correct information and tools among the many sources of information, we recommend to:

- Collectively create one central webpage with all relevant information for researchers. This is currently being created in the form of the Data Privacy Handbook, initiated by the RDM Support team. Ideally, similar content that currently exists on other UU-related websites can be consolidated in the Data Privacy Handbook in consultation with those responsible for such websites.
- Communicate the UU-specific procedures and templates applicable to researchers via the UU intranet.
- Actively educate researchers on the basics of handling personal data at UU through trainings, workshops, and in-person contact. Currently, a privacy awareness training is being developed for all UU employees. For researchers specifically, a course tailored to research, and including where to go for help, may be more valuable to support them in their daily work. Currently, RDM Support is working on an online course that can fulfill this function, to be launched before the summer of 2023.

### 4.4 Increase the hands-on nature of support

A selection of researchers indicated to have bad experiences with data support staff in the past. To prevent this from happening in the future, we recommend all data support staff to:

- Reduce the use of legal terminology to a minimum when advising researchers. Privacy and security officers should at least have a basic understanding of the process of performing research and the common issues within it.
- Consistently collaborate with other data support staff within and beyond the faculty to find quick solutions to researchers' problems, and prevent projects from dragging on.
- Increase personal contact with researchers, for example by visiting departmental meetings, adding names (and/or faces) to general email addresses, providing regular (in-person) privacy-related trainings, and maintaining direct contact with department heads. As shown by the fact that many respondents consult with colleagues for information and support, personal contact with data support staff will likely be more effective at increasing awareness and compliance than a passive website. A proactive approach of privacy officers and data managers is therefore desirable.

### 4.5 Improve the quality of information and tools

As stated above, in case researchers were able to locate the correct information resource and tools, they did not always experience those as being helpful. We therefore recommend to:

- Develop tools and concrete information, answering frequently asked questions concretely (e.g., what is personal data, when are data anonymous, what do students have to do with privacy, how to properly share data, etc.). This is currently being tackled within the Data Privacy Handbook.
- Provide ready to use templates and examples for different research scenarios. For example, many DPIAs or Privacy scans may be similar across different research projects, and imply similar safeguards. Adapting existing examples (using similar safeguards) instead of starting from scratch will greatly speed up the process for both data support staff and researchers. There is a role here for both RDM Support and privacy officers, ideally within the same Data Privacy Project.