Data Privacy Handbook

Utrecht University

2021-11-05

Contents

Welcome! **7**

0.1 How to use this Handbook 8

0.2 License and Citation 9

0.3 Disclaimer 9

0.4 Contributions 10

I Knowledge Base **11**

The GDPR & Research Data **13**

Legal Basis for Processing Data 13

0.5 Reusing Privacy-Sensitive Data 13

0.6 Data Subject's Rights 13

1 Privacy & Security Assessment **15**

2 Legal Documents & Agreements **17**

2.1 Privacy Notices 17

2.2 Informed Consent Forms 17

2.3 Data Use Agreement/Confidentiality Agreement/Non-Disclosure Agreement 17

2.4 Data Transfer Agreement 17

2.5 Consortium Agreement and/or Joint Controller Agreement . . . 17

2.6 Data Processing Agreement 17

II Techniques & Tools **19**

3 Privacy-Enhancing Techniques in Working With Personal Data **21**

3.1 Anonymization 21

3.2 Pseudonymization 21

3.3 Encryption 21

3.4 Synthetic Data 21

3.5 Federated Analysis 21

4 Tools & Services **23**

4.1 tools.uu.nl 23

4.2 Survey Tools 23

4.3 Transcription Tools 23

III Storage, Sharing, Publication **25**

5 Data Storage **27**

5.1 Network Drives 27

5.2 Cloud Drives 27

5.3 Hard Drives 27

6 Data Sharing **29**

6.1 Can I Share Personal Data? 29

6.2 Third Country Transfers 29

6.3 Data Access Protocols 29

6.4 Data Points/Virtual Research Environments 29

7 Data Publishing **31**

7.1 Publishing Personal Data 31

7.2 Data vs. Metadata 31

7.3 Repositories 31

7.4 Licenses 31

8 (PART) Use Cases **33**

9 Open Science Questionnaire: publishing metadata **35**

10 YOUth Cohort Study: Data pseudonymisation **37**

11 YOUth Cohort Study: Data sharing outside of EEA **39**

12 UU Employee study: Creating fake data to safely test analysis scripts **41**

Welcome!

Utrecht University

Data Privacy Handbook

The Data Privacy Handbook is a guide on handling personal data in scientific research, in line with European data protection and privacy regulations. It consists of:

- A **knowledge base** which explains how the EU General Data Protection Regulation (GDPR, Dutch: Algemene Verordening Gegevensbescherming) applies to scientific research, including guidelines and good practices in carrying out GDPR-compliant scientific research;
- An overview of privacy-enhancing **techniques & tools** and practical guidance on their implementation;
- **Use Cases** in the form of research projects with privacy-related issues, for which a reusable solution (e.g., tool, workflow) has been developed.

The Data Privacy Handbook synthesizes information across various sources and presents it a *practical* and *actionable* format. This includes workflows, tools, and practical translations of the GDPR , which could be used by researchers and (data) support staff within Utrecht University and beyond.

This is an Utrecht University (UU) community-driven, open-source project. You can visit our GitHub repository here. We welcome feedback and contributions of any type, please read our contributing guidelines for more information.

The Data Privacy Handbook is an initiative of Research Data Management Support at the Utrecht University Library, in collaboration with privacy and data experts at Utrecht University. It is part of a larger Data Privacy Project, that aims to develop knowledge, tools, and experience on how researchers can and

should deal with personal data. This project is funded by the Utrecht University Research IT Program and an NWO Digital Competence Center grant. You can read more about the Data Privacy Project here.

0.1 How to use this Handbook

The Data Privacy Handbook aims to make knowledge and solutions on handling personal data *Findable, Accessible, Interoperable, and Reusable* (FAIR) and present them in a practical and actionable format.

The Handbook need not be read like a textbook. You are invited to navigate to the topic you need based on the table of contents, or use the guide below.

0.1.1 What are you looking for?

I want to…:

Learn about the GDPR in the context of scientific research

Introduction to the GDPR

Definitions

Plan a GDPR-compliant research project

Assessing your design

Informing participants

Obtaining consent

Collaborating on personal data

Work safely with personal data

Storing personal data

Using GDPR-compliant tools and services

Reducing the sensitivity of personal data

Sharing personal data during research

Share personal data with others

Sharing data legally

Sharing personal data during research

Reducing the sensitivity of personal data

Using GDPR-compliant tools and services

Publishing personal data

Sharing personal data case by case

Learn from other projects

Publishing metadata only

Pseudonymising different types of data

Sharing personal data outside of the EEA

Creating fake data to test analysis scripts

Get help or information

Getting help at Utrecht University

Definitions

References

0.2 License and Citation

0.2.1 Citing the Data Privacy Handbook

To be announced.

0.3 Disclaimer

The content presented in the Data Privacy Handbook has been carefully curated by Research Data Management Support, in collaboration with privacy officers and data experts of Utrecht University.

The Data Privacy Handbook is a 'living' book that is continually being written, updated and reviewed. Its contents can therefore change, or become outdated or redundant . Hence, the information presented is provided "as is", **without guarantees of accuracy or completeness**.

As scientific research may differ depending on the discipline, topic, and context, measures needed or taken to ensure GDPR-compliance will vary across research projects. The authors can therefore **not be held responsible, nor accountable** for any negative consequences arising from interpretation and use of the content of the Data Privacy Handbook.

The Handbook is not endorsed by the Board of Utrecht University and does not constitute a mandatory directive. For the most up-to-date and

official/authoritative information, please refer to the university website and intranet, to which this Handbook is a hands-on, practical supplement. Moreover, before implementing the guidance laid out in this Handbook, always seek the advice of your privacy officer or RDM Support to confirm the suitability of any proposed solution to your project.

Throughout the Data Privacy Handbook, links to external webpages may be provided for additional information or assistance. The authors of the Data Privacy Handbook are **not responsible for the content of any such linked webpages**, nor is the content of external webpages necessarily endorsed by Utrecht University.

Utrecht University is committed to sharing knowledge in line with the principles of open science and therefore welcomes readers from outside of the organization. However, the contents of the Data Privacy Handbook may not be in line with readers' institutions' policies or views. For more authoritative information, these readers' should refer to resources from their own institutions.

0.4 Contributions

The Data Privacy Handbook is a collaborative effort, made possible by a large number of contributors (also to be viewed in our GitHub repository):

Neha Moopen, Dorien Huijser, Jacques Flores, Saskia van den Hout, Frans Huigen, Sanne Kleerebezem, Annemiek van der Kuil, Danny de Koning-van Nieuwamerongen, Frans de Liagre Böhl, Francisco Romero Pastrana, Ron Scholten, Garrett Speed, Robert Steeman, Liliana Vargas Meleza, Martine de Vos, and others.

Would you like to contribute to this Handbook yourself? Please read our Contributing Guidelines.

Part I

Knowledge Base

The GDPR & Research Data

This chapter may include sections on the legal basis for processing research data, reusing privacy-sensitive data (further processing), and data subject's rights.

Legal Basis for Processing Data

0.5 Reusing Privacy-Sensitive Data

0.6 Data Subject's Rights

0.6.1 Right to be Informed

0.6.2 Right to Access

0.6.3 Right to Erasure

0.6.4 Right to Rectification

Chapter 1

Privacy & Security Assessment

Chapter 2

Legal Documents & Agreements

2.1 Privacy Notices

2.2 Informed Consent Forms

2.3 Data Use Agreement/Confidentiality Agreement/Non-Disclosure Agreement

2.4 Data Transfer Agreement

2.5 Consortium Agreement and/or Joint Controller Agreement

2.6 Data Processing Agreement

Part II

Techniques & Tools

Chapter 3

Privacy-Enhancing Techniques in Working With Personal Data

3.1 Anonymization

3.2 Pseudonymization

3.3 Encryption

3.4 Synthetic Data

3.5 Federated Analysis

Chapter 4

Tools & Services

4.1 tools.uu.nl

4.2 Survey Tools

4.3 Transcription Tools

Part III

Storage, Sharing, Publication

Chapter 5

Data Storage

5.1 Network Drives

5.2 Cloud Drives

5.3 Hard Drives

Chapter 6

Data Sharing

6.1 Can I Share Personal Data?

6.2 Third Country Transfers

6.3 Data Access Protocols

6.4 Data Points/Virtual Research Environments

Chapter 7

Data Publishing

7.1 Publishing Personal Data

7.2 Data vs. Metadata

7.3 Repositories

7.4 Licenses

Chapter 8

(PART) Use Cases

Chapter 9

Open Science Questionnaire: publishing metadata

Chapter 10

YOUth Cohort Study: Data pseudonymisation

Chapter 11

YOUth Cohort Study: Data sharing outside of EEA

Chapter 12

UU Employee study: Creating fake data to safely test analysis scripts

The glossary will consist of frequently used jargon concerning the GDPR and research data.