Research Data Guide

Faculty of Religion and Theology

1. Starting Out: Assessment & the DMP	
What are the types of data to be collected, processed and stored? - E.g., documentary data, photographs, graphs, audio, scans, data from historical archives, survey data, social media data, observational data, field notes, etc. What security, privacy or access requirements does your data have? ➤ All data must comply with the GDPR: https://libguides.vu.nl/rdm/gdpr-privacy ➤ Do you (re)use personal data? (i.e., any information relating to an identifiable, living individual). ➤ If so, you will need ethical clearance. Contact: research.bureau.frt@vu.nl ➤ How many people/institutions will need access to the data? Will different levels of access/clearance be needed. ➤ How often will the data be altered/processed? ➤ What volume of storage will you require? You will need to answer the above questions in the DMP. **DMP (Data Management Plan)** ➤ You are required to fill in a DMP (Data Management Plan). The VU offers an online tool for this: *DMPOnline.* Select a template and fill it in according to the instructions: https://dmponline.vu.nl/ ➤ The DMP is meant to be a **living document**, it does not need to be "complete."	💡 *"But I do not collect or use any data."* Whether you deal with historical texts or interviews, it is all data. 💡 *"What format should my data be in?"* Ensure that you choose a format that is open-source, well-documented, accepted in the field, and not compressed. (e.g., *pdf, txt, xml* not *docx*; *wav* not *mp3*).
2. Starting Out: Choosing Data Storage	
It is important to choose the correct place to store your data. This depends on the type, volume, security, privacy, and access requirements of your data. **Choosing data storage for your project** - It is not sufficient to use free cloud services such as Google Drive or Dropbox (VU has no agreements), a personal laptop, or a USB-drive for research data. Hardware is not allowed as it's not safe or secure. - Instead, a number of options are available, these include YODA, Research Drive, and SciStor. They are project based. The VU's storage finder is very helpful in selecting one: https://vu.nl/en/research/storagefinder	💡 *"I am an external / I do not have a VUnetID."* You can contact your supervisor to apply for a VUnetID for you. You can also gain access to YODA (*see below*). External PhD's have to send an email to the Graduate School to acquire a Yoda account. The Graduate School will take care of the access to Yoda.

• OneDrive and SURFDrive are secure and suitable for your own data, not for project data. They are tied to you, not the project, and will be erased when you leave VU. // **Note**: OneDrive can be used for project data if you have no sensitive data (e.g., only lit. review).	💡 *"Can I store my data in an external/secondary institution?."*
• For sensitive data a secure storage facility is needed: YODA or Research Drive is recommended.	To use external storage it needs to have a processing and/or collaboration agreement with the VU. It is also important which university is the data controller. For more information about the processing and/or collaboration agreement please contact the Research Bureau FRT: research.bureau.frt@vu.nl
➢ Which to choose? *In addition to being very secure, YODA's advantage is that it allows data archiving at the end of the project, while Research Drive's advantage is that it allows the setting of different access-levels to sections of the project/data (e.g., if not everyone needs access to all parts).*	
• If you are unsure which storage to choose, contact FRT's data steward at rdm.frt@vu.nl or utilize the VU's storage finder (linked above).	💡 *"I do not have access to (X) storage."* Contact FRT's data steward, or the central RDM desk at: rdm@vu.nl *For YODA access (takes a few days): Requesting storage space, costs (vu-rdm-tech.github.io)
3. During the Project: Secure/FAIR Data Practices	
• When sending files a secure sharing system should be used, such as SURFfilesender or ZIVVER. See: https://libguides.vu.nl/rdm/data-storage	💡 *"I need to receive files from someone not from the VU."*
• Basic data security should be followed (e.g., data should not be stored on personal hardware, or left unattended.)	SURFfilesender can be used to securely receive files from non-VU or international colleagues (e.g., setting up a file drop folder). See: https://libguides.vu.nl/rdm/data-protection
• Consent Forms: Use digital forms when possible. Survey tools such as Qualtrics can be used.	
• You may wish to de-identify (pseudonymize, or anonymize) any personal data collected. See: https://fgb-rdm.nl/Security/Deidentification.html	💡 *"But I had already started collecting data."*
• Encrypt extra sensitive data (e.g., your pseudonymization key, raw sensitive interview footage, etc.). You can use Cryptomator: https://cryptomator.org/	If you had already started collecting data, secure it and be sure to transfer it to your chosen secure storage as soon as you gain access. Please note that de collection of personal/sensitive data can only start when the CWBE (ethical committee) has formally given a positive advice. Contact
• Follow FAIR data principles (findable, accessible, interoperable, reusable). See: https://www.go-fair.org/fair-principles/	

➢ This is important for research integrity and impact. • Review your DMP and update it as you go along.	the Research Bureau if you need an ethical clearance: research.bureau.frt@vu.nl

4. After the Project: Archiving & Documentation	
After project completion, all research data is required to be archived for 10 years in a trusted repository. Any data that is not published will go to a repository. A good data repository will do these three things: 1. Provide a persistent, unique identifier (PID). *This is critical for data discovery – it enables searching, citing and retrieval of your data, and versioning.* 2. Contain adequate metadata standards. *Metadata is data about your data. A good repository will have standardized, machine-readable metadata.* 3. Data access and licensing. *A good repository will enable access to your data depending on well-specified conditions.* **What are my archive options at the VU?** • **YODA**: It has a dedicated archive for all <u>sensitive data</u>. Provides a PID. Metadata is published. Access can be tailored. (*All GDPR-compliant personal data at the VU should go here*). Yoda - VU - Home • **DataverseNL**: Not suitable for *very* sensitive data. Provides a PID. Access can be tailored. See: https://dataverse.nl/dataverse/vuamsterdam • **Open Science Framework** (OSF): Not suitable for sensitive data. Provides a PID. Open-access. See: https://osf.io/abwzm/ • **External Repositories**: DANS Data Stations (Manual depositing data | DANS (knaw.nl)), 4TU Research Data, Zenodo, or discipline-specific repositories. **Things to consider:** • Add data documentation and metadata (data about your data). See: https://libguides.vu.nl/rdm/metadata • All data that is sensitive will be archived, all data that is not sensitive should be published "*as open as possible, as closed as necessary*." • Consider what licensing to use. For publishing/licensing advice, see: https://libguides.vu.nl/rdm/data-publication	*What is a PID? How may I get one?* • A Persistent Identifier (PID) is a digital identifier for a person, project or institution. See: Persistent identifiers and data citation explained • For projects this is often a DOI (Digital Object Identifier). Good repositories will provide this. • For researchers, ORCID provides a personal identifier that you own. We recommend everyone have an ORCID (can be linked to PURE). You can set it up in 10minutes: ORCID - Vrije Universiteit Amsterdam (vu.nl) If you are unsure which archive to choose, contact FRT's data steward at rdm.frt@vu.nl