

Data Management Plan for SNSF research projects

General guidelines

Contents

Introduction	3
1. General information	4
1.1. When to prepare a DMP	4
1.2. Data details	4
1.3. Metadata	4
1.4. Data storage and data treatment	5
1.5. Data preservation	5
1.5.1. Data selection	5
1.5.2. Formats of data for long-term preservation	6
1.6. Data sharing	6
1.6.1. Personal and sensitive data	6
1.6.1.1. Swiss law	7
1.6.1.2. European law: GDPR	7
1.6.1.3. Informed consent	8
1.6.2. Licenses	8
1.7. Data repositories	9
2. DMP for SNSF projects	11
2.1. Preparation of the DMP	11
2.2. Structure of the DMP	11
Contacts	15

Introduction

The aim of a Data Management Plan is to plan and manage the whole life cycle of data¹. It offers a long-term perspective by outlining how data will be generated, collected, documented, shared and preserved.

Managing and sharing research data as openly as possible is one of the principles of good scientific practice. Following the SNSF Funding Regulations (Article 47) *“During the course of the research work and after its completion, grantees are obliged to make available to the public in an appropriate manner the research results obtained with the help of SNSF funding, thereby explicitly mentioning the support obtained from the SNSF”*.

Similarly, beneficiaries of EU funding are expected to share their data according to the FAIR Data principles, meaning that data should be Findable, Accessible, Interoperable and Reusable².

In Chapter 1 you will find general information on data and data management. Chapter 2 provides details on the SNSF Data Management Plan as well as its structure and required content.

These guidelines are complemented by a series of DMP example that the user may find at the dedicated USI Research and Transfer Service (SRIT) [website](#).

¹ Data life cycle: data management planning – data acquisition – data annotation – data processing – data analysis – data documentation and preservation – data publication and sharing (archiving) – data reuse.

² [FAIR principles detailed](#)

1. General information

1.1. When to prepare a DMP

The preparation of a DMP should start during the project-planning phase. At this stage it is an useful instrument to properly plan your data creation and analysis, as well as to address relevant issues related to data storage and data sharing. Nevertheless, the DMP is a living document that remains editable for the whole duration of a research project. Information can be specified or updated accordingly to the project progresses. At the latest the DMP should be revised by the end of the project in view of the data preservation, publication and reuse. For further information on SNSF deadlines for the DMP, see [§2.1](#).

As far as academic disciplines are concerned, the compilation of a DMP is flexible and each scientific community may define its own standard. In general, the best way of planning the management of research data may vary from field to field.

1.2. Data details

Research data are data collected or produced in the course of scholarly activity which are used for the purposes of academic research or which document research findings.

In the DMP it is important to detail the specifics (data type, data origin, data formats, files formats, etc.) of each dataset that is going to be part of the research, and whether they are generated ex-novo or reused from a third party. Another major aspect concerns the indication of the estimated data volume, more so when this is expected to reach important sizes (see [§1.4](#)).

One important aspect regards the definition of data. According to the [Swiss National Open Research Data Strategy](#), “research data” have to be understood in a broad sense. The Strategy is concerned with data in the form of digital objects that are required for the reuse of data themselves and reproduction of research results. Thus, “research data” also includes generated and/or implemented codes and algorithms necessary to reproduce and validate the results of the research/publication.

1.3. Metadata

Metadata is documentation that describes all relevant information regarding data. Properly describing and documenting data allows users (yourself included) to understand and track important details of the work, making it is easy to interpret how data was generated and the context of data. The importance of metadata resides in the general concept that research data should be made available for reuse (also according to FAIR principles) and that research findings should be reproducible, enhancing effectiveness of the research process. Also, metadata should be compiled in order to make data findable meaning that it should consist of attributes that ease the process of searching, querying, mining and in general accessing the database. Hence, a precise and correct compilation of metadata documentation is of utmost importance.

Metadata contains generally descriptive information like the creator, date and subject of the dataset, information that tells how the dataset relates to other documents and information on the format, access rights or preservation aspects.

It is important to capture this information right from the start of the project. Sometimes metadata is embedded in the dataset as it is automatically created by the software or tool that generates the data. If not, metadata can be registered in a separate file, like a README.txt, .csv spreadsheet or .xml document. As a general rule, in order to grant interoperability it is good practice that metadata is rendered machine-readable, hence metadata should be stored in standardised formats that can be used and understood by a computer. One should also specify information concerning the software (including its version) used to produce and treat data. Also, many academic disciplines have formalized specific metadata standards and it is good practice to conform to them. If no appropriate

standard is available, the applicant should describe the ad hoc metadata that is going to be adopted. You can check out formalized metadata standards on the [Digital Curation Center](#) website. Another list is provided by the [research data Alliance](#).

1.4. Data storage and data treatment

It is good practice to adopt an organized scheme in order to stock and organize the research data as well as to monitor the changes that may occur in the databases during their lifetime. For example, one may want to define in advance a naming convention and a folder structure to organize data and, if necessary, adopt a code revision management system (or version control software) such as [Git](#).

Institutional server space is available to USI researchers in which project data can be stored and treated. File servers are managed by IT services and are protected by backup copies of data made every night of working days.

It is good practice to indicate in advance the tools one intends to adopt in order to treat the data. There are cases in which applicants are going to need significant computing resources (e.g., High-Performance Computing as performed by CSCS), special software/hardware (e.g. dedicated server clusters, racks) and/or very large server space in order to stock data and perform the necessary analyses in the context of their research project. We strongly recommend applicants that anticipate such needs to get in touch beforehand with the USI Research Data Manager (igor.sarman@usi.ch) and the IT team dealing with these matters (serviceportal.usi.ch), as well as to detail such needs in their DMPs.

1.5. Data preservation

By the end of the project you have to decide which of your research data should be preserved and how. In this sense, it is important to describe the procedure to be adopted to grant data preservation. If possible, research data should be archived and published in a dedicated data repository (see [§1.6](#) and [§1.7](#)). It might occur that some data cannot be made publicly available (data preservation does not necessarily mean data publication) and should be preserved only on institutional file servers with restricted access. In both cases data preservation must be properly planned.

Personal and sensitive data should be handled and preserved in line with the relevant legal framework and informed consent (see [§1.6.1.3](#)).

1.5.1. Data selection

It is not always feasible nor appropriate to preserve all data used in the context of a research project. You might want to focus on the following:

- data which are needed to validate research findings;
- data that cannot easily be recreated or produced;
- data that is expensive to reproduce;
- experimental data;
- third party or acquired data for which the future availability is uncertain;
- data needed for further reuse.

In addition, you should also consider whether you will need to preserve multiple versions of a file or whether the most recent version will be sufficient for preservation. Furthermore, you should report what data elaborations will be applied (i.e. data anonymization when dealing with personal and sensitive data) and what measures will be put in place to grant accessibility.

You also have to consider for how long the data should be preserved. In general, it is best to commit to a minimum amount of time than a maximum. However, there is no fixed amount of time for which data must be preserved. A good practice to establish a minimum amount of time may be to consider the amount of time it takes for a research paper to be cited and then to add 5 years.

It is also useful to set a timeframe after which the preservation of your research data should be re-evaluated.

1.5.2. Formats of data for long-term preservation

Since hardware and software may become obsolete over time, data should be converted into standard or open formats for long-term accessibility and preservation. The following table provides a list of appropriate data formats that you may want to prefer and formats that you should try to avoid for data preservation:

Type of data	Appropriate	Acceptable	Not suitable
Tabular data with extensive metadata	.csv, .hdf5	.txt, .html, .tex, .por	
Tabular data with minimal metadata	.csv, .tab, .ods	.xml, .xlsx, SQL script	.xls, .xlsb
Textual data	.pdf, .txt, .odt, .odm, .tex, .md, .htm, .xml	.pptx, .pdf with embedded forms, .rtf, docx	.doc, .ppt
Code	.m, .R, .py, .iypnb, .rstudio, .rmd, NetCDF	.sdd	.mat, .rdata
Digital image data	.tif, .png, .svg, .jpeg	.jpg, .jp2, .tif, .tiff, .odf, .gif, .bmp	.indd, .ait, .psd
Digital audio data	.flac, .wav, .ogg	.mp3, .mp4, .aif	
Digital video data	.mp4, .mj2, .avi, .mkv	.ogm, .webm	.wmv, .mov
Generic data	.xml, .json, .rdf		

1.6. Data sharing

Research data should be shared as soon as possible, but at the latest together with the relevant scientific publication. The SNSF expects that data generated by funded projects are publicly accessible in digital databases provided there are no legal, ethical, copyright or other issues. Besides responding to public requirements, sharing your data helps generating more visibility to your research.

Datasets must always be carefully documented with associated metadata, such that other researchers understand how the data was collected, as well as under which conditions and how it can be re-used (see [§1.3](#)).

The FAIR Data Principles define a range of qualities a published dataset should have in order to be Findable, Accessible, Interoperable and Reusable (see [FAIR Data Principles](#) as explained by SNSF). The SNSF as well as the EU expects researchers to share their data according to the FAIR Data Principles on publicly accessible, digital repositories. It is important to note that the FAIR Data Principles do not require researchers to share all their data without any restriction. The general idea that should guide researchers when sharing data is “as open as possible, as closed as necessary” as illustrated by the FAIR principles. In cases where data cannot be shared because of legal, ethical, copyright, confidentiality or other clauses, applicants are asked to clarify the specific limitations. In case of third-party data reuse, one has to verify if restrictions to data dissemination are in effect. If third-party data can be shared, this has to be done according to the original requirements and licenses.

1.6.1. Personal and sensitive data

Personal data is all information relating to an identified or identifiable person (Swiss FADP³, article 3 a.), such as name, address, identification number, e-mail, phone number, medical records, etc.

³ Federal Act on Data Protection.

Sensitive data, according to the Swiss FADP (article 3 c.) is data on:

- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or the racial origin;
- social security measures;
- administrative or criminal proceedings and sanctions.

Working with personal/sensitive data may pose important ethical issues that have to be detailed in the DMP. It is necessary to describe how ethical issues will be managed across the entire lifespan of data as well as what data protection measures will be implemented to avoid unauthorized access to data. Before collecting personal/sensitive information the researcher has to put in place the procedures to obtain informed consent. Access to personal/sensitive data has to be restricted, storage must occur in a safe location ([§1.4](#)) and transfer of data between research partners must be performed under protective measures. In order to protect personal and sensitive data you must anonymize your datasets before publication in such a way that it will be impossible to retrace individuals. Anonymization has to be irreversible; data identifiers need to be removed, generalised, aggregated or distorted. Anonymous data are not considered as personal data since they do not correspond to an identified or identifiable person.

Data pseudonymization is instead a method of de-identification that replaces identifiers with pseudonyms or identifiers that are generated by the researcher. Using pseudonyms allows researchers to link de-identified data to the same individual across multiple datasets while retaining confidentiality of the individual. This means that, unlike anonymized data, pseudonymized data can be linked across datasets. Linking across datasets can make data more useful, but it can also increase the risk of re-identification.

1.6.1.1. Swiss law

In Switzerland, the processing of personal and sensitive data is subject to the [Federal Act on Data Protection](#) and to cantonal laws.

The collection of personal and sensitive data is only possible with prior and informed consent of the person concerned or when such collection is explicitly provided for in the law. Unless anonymised, the data may be processed only for the purpose indicated at the time of collection.

The Swiss law on data protection is currently under revision, also in order to better align with the European law (GDPR), and is expected to entry into force in 2022. Please note that European law (GDPR) is more demanding in terms of consent and data protection, we therefore suggest to always take into account the European legal framework when dealing with personal data (see next section).

1.6.1.2. European law: GDPR

The [General Data Protection Regulations](#) (GDPR) regulate data protection and privacy for any individual residing within EU, as well as the communication of personal data outside EU. In the field of research, this regulation applies to all institutions and companies operating internationally that collect and process personal data of EU residents or send data from Swiss nationals abroad.

Complying with GDPR is a good practice for all research projects, regardless of the source and use of data.

Personal data may only be collected for specified, explicit and legitimate purposes, which should in principle be defined prior to processing and brought to the attention of the data subjects. GDPR requires that in case of collection and processing of personal data, consent must be expressed freely and explicitly. Therefore Consent will only constitute an appropriate legal basis if the person concerned has a real control and choice as to whether or not to accept the proposed conditions or to refuse them without prejudice.

1.6.1.3. Informed consent

If you are working with persons' data, you should confirm the following⁴:

- have the subjects of your data collection (persons) been fully informed (what data do you collect, what will you do with the data, and who will receive it; when will they be deleted) and have the subjects given their informed consent?
- have the subjects of your data collection (persons) been informed about their rights on information, data deletion and data correction?

Following the European law, informed consent is required for the processing of personal and sensitive data and must fulfill the following criteria:

- **Free:** the person must not feel compelled to consent and his or her consent must not be conditional on the granting of an advantage.
- **Specific:** consent must be obtained for each purpose and not for a set of purposes.
- **Informed:** the person must be informed on the identity of the controller, the purposes of the processing operation, the legal bases, etc.
- **Unambiguous:** consent must be given by a clear positive act. The controller must then keep proof of the given consent.

A template of the informed consent can be requested to the USI Research and Transfer Service. Further guidelines are provided by [FORS](#).

1.6.2. Licenses

A license clarifies the terms of use of your work allowing you to share your data with the proper protection. By default, a work with no license is a copyrighted work (all right reserved). Attaching a license to a publicly accessible dataset allows to explicitly clarify what can legally be done with it.

A Creative Common (CC) license is one of several public copyright licenses that enable free distribution of an otherwise copyrighted work. It is used when an author wants to give other people the right to share, use and build upon a work that he has created. Please find below an explanation of different CC licenses, from the most open to the most restrictive:

License	Right	Description
CC0	Free	Completely free.
CC-BY	Attribution	Licensees may copy, distribute, display and perform the work and make derivative works and remixes based on it only if they give the author or licensor the credits (attribution).
CC-BY-SA	Attribution Share-alike	Attribution + Licensees may distribute derivative works only under a license identical ("not more restrictive") to the license that governs the original work.
CC-BY-NC	Attribution Non commercial	Attribution + Licensees may copy, distribute, display, and perform the work and make derivative works and remixes based on it only for non-commercial purposes.
CC-BY-NC-SA	Attribution Non commercial Share-alike	See above.
CC-BY-ND	Attribution No derivative works	Attribution + Licensees may copy, distribute, display and perform only verbatim copies of the work, not derivative works and remixes based on it.
CC-BY-NC-ND	Attribution Non commercial No derivative works	See above.

⁴ [Data Life Cycle Management \(DLCM\) guidelines](#)

1.7. Data repositories

The public funding bodies require grantees to publish their data in non-commercial data repositories complying with the FAIR data principles. You are free to choose field-specific repositories (e.g. PubMed Central for Life Sciences or ArXiv for Engineering) or repositories that accept datasets from different research fields.

Publication of data and outputs on data repositories must comply with the respective legal framework (Intellectual Property Rights, licenses, informed consent, data ownership, etc.). Most of the scientific journals set an embargo period after which you are entitled to publish a specified version of your article in a FAIR repository. Check the journal's policy on <http://www.sherpa.ac.uk/romeo>.

In order to facilitate the identification of a FAIR repository, the SNSF guidelines for DMP present a checklist defining the minimum criteria for a repository to be considered FAIR. For this purpose, the answer to all the questions below must be "yes":

- Are datasets (or ideally single files in a dataset) given globally unique and persistent identifiers (e.g. DOI)?
- Does the repository allow the upload of intrinsic (e.g. author's name, content of dataset, associated publication, etc.) and submitter-defined (e.g. definition of variable names, etc.) metadata?
- Is it clear under which licence (e.g. CC0, CC BY, etc.) the data will be available, or can the user upload/choose a licence?
- Are the citation information and metadata always (even in the case of datasets with restricted access) publicly accessible?
- Does the repository provide a submission form requesting intrinsic metadata in a specific format (to ensure machine readability/interoperability)?
- Does the repository have a long-term preservation plan for the archived data?

Please find below a list of four repositories which accept datasets from different fields and fulfil the funder's requirements⁵:

Repository	License	Metadata	Other
Zenodo	Default is CC-BY, but user can choose different license or restrict the access and set a condition.	Always publicly available (also in case of restricted access).	Allows to easily publish or cite a GitHub repository (link).
Harvard Dataverse	Default is CC0 waiver, but custom terms of use can be specified.	Always publicly available (also in case of restricted access).	
Eudat	Licenses for datasets are chosen by submitters and defined via an online form.	Always publicly available (also in case of restricted access).	
Dryad	All data submitted to Dryad are released to the public domain under CC0.	Always publicly available.	Dryad only accepts human subject data that is properly anonymized and prepared under applicable legal and ethical guidelines.

In case of doubt, we recommend to visit the page www.re3data.org where most research data repositories are listed. This page is also useful when a repository is deemed as commercial. In this case the following procedure may be considered:

- Under the tab "Institutions", check if a commercial entity is involved in 'general' or 'technical' responsibility (categories "Type of institution" and "Type(s) of responsibility")

⁵ A detailed description of how these four repositories comply with the checklist can be found [here](#)

- If not, SNSF considers the repository to be non-commercial (even if 'funding' or 'sponsoring' is provided by a commercial entity).
- If yes, the SNSF considers the solution to be a commercial repository (see [details](#))

If the repository is not listed on www.re3data.org, the repository should be contacted to clarify this point.

2. DMP for SNSF projects

2.1. Preparation of the DMP

The DMP is an integral part of the grant proposal and the proposal can only be submitted once the DMP has been completed⁶. Following the SNSF Guidelines, at the stage of grant proposal the DMP is considered a draft and excluded from the scientific evaluation process (DMPs are not sent out for external review). The submitted DMP is considered as a notice of intention, its content is assessed by the SNSF Administrative Offices for its plausibility and compliance to the SNSF policy on open research data. If there are shortcomings in the submitted information, applicants will have to complete/amend specific sections of the DMP at the time of the funding decision and at the latest by the request for release of funds. The DMP remains editable during the entire lifetime of the grant and the final version has to be provided by the end of the project at the latest. In this final version, which will be assessed together with the final scientific report, the SNSF expects that the management of the data, which was collected, generated and observed during the course of the project, is described conclusively.

The formal structure of SNSF DMP is detailed in section [§2.3](#). It is important to notice that depending on the project and research field not all the questions in the DMP have necessarily to be addressed, in this case it would be good practice to explain the rationale. Similarly, some research projects do not produce or reuse any data. In this case applicants are not expected to complete the whole DMP form and they are asked to explain why they do not plan to generate or reuse any data in their proposed research.

The costs of enabling access to research data that is collected, observed or generated under an SNSF grant should be included in the project budget. Such costs must be related to the preparation of research data in view of its archiving or to the archiving itself in a FAIR data repository that do not serve commercial purposes⁷. The maximum charge per grant is CHF 10'000⁸.

2.2. Structure of the DMP

In your grant application form on mySNF you will find the following questions in the DMP section. Short but comprehensive answers for each of them are required.

1. Data collection and documentation

1.1. What data will you collect, observe, generate or reuse?

Briefly describe the data you will collect, observe or generate. Also mention any existing data that will be (re)used. The descriptions should include the type, format and content of each dataset. Furthermore, provide an estimation of the volume of the generated data sets. (This relates to the [FAIR Data Principles](#) F2, I3, R1 & R1.2)

*What type, format and volume of data will you collect, observe, generate or reuse?
Which existing data (yours or third-party) will you reuse?*

See [§1.2](#).

1.2. How will the data be collected, observed or generated?

Explain how the data will be collected, observed or generated. Describe how you plan to control and document the consistency and quality of the collected data: calibration

⁶ [SNSF Data Management Plan \(DMP\) - Guidelines for researchers](#)

⁷ [General implementation regulations for the Funding Regulations, subchapter 2.13](#)

⁸ The SNSF also covers the costs of scientific open access publications. One may find further information concerning the Open Access policies and practices at USI at the dedicated webpage of [USI Library](#)

processes, repeated measurements, data recording standards, usage of controlled vocabularies, data entry validation, data peer review, etc. Discuss how the data management will be handled during the project, mentioning for example naming conventions, version control and folder structures. (This relates to the [FAIR Data Principle R1](#))

*What standards, methodologies or quality assurance processes will you use?
How will you organize your files and handle versioning?*

1.3. What documentation and metadata will you provide with the data?

Describe all types of documentation (README files, metadata, etc.) you will provide to help secondary users to understand and reuse your data. Metadata should at least include basic details allowing other users (computer or human) to find the data. This includes at least a name and a persistent identifier for each file, the name of the person who collected or contributed to the data, the date of collection and the conditions to access the data. Furthermore, the documentation may include details on the methodology used, information about the performed processing and analytical steps, variable definitions, references to vocabularies used, as well as units of measurement. Wherever possible, the documentation should follow existing community standards and guidelines. Explain how you will prepare and share this information. (This relates to the [FAIR Data Principles I1, I2, I3, R1, R1.2 & R1.3](#))

What information is required for computer or humans to read and interpret the data in the future?

How will you generate this documentation?

What community standards (if any) will be used to annotate the (meta)data?

See [§1.3](#).

2. Ethics, legal and security issues

2.1 How will ethical issues be addressed and handled?

Ethical issues in research projects demand for an adaptation of research data management practices, e.g. how data is stored, who can access/reuse the data and how long the data is stored. Methods to manage ethical concerns may include: anonymization of data; gain approval by ethics committees; formal consent agreements. You should outline that all ethical issues in your project have been identified, including the corresponding measures in data management. (This relates to the [FAIR Data Principle A1](#))

What is the relevant protection standard for your data? Are you bound by a confidentiality agreement?

Do you have the necessary permission to obtain, process, preserve and share the data? Have the people whose data you are using been informed or did they give their consent?

What methods will you use to ensure the protection of personal or other sensitive data?

See [§1.5.1](#).

2.2. How will data access and security be managed?

If you work with personal or other sensitive data you should outline the security measures in order to protect the data. Please list formal standards which will be adopted in your study. Furthermore, describe the main processes or facilities for storage and processing of personal or other sensitive data. (This relates to the [FAIR Data Principle A1](#))

What are the main concerns regarding data security, what are the levels of risk and what measures are in place to handle security risks?

How will you regulate data access rights/permissions to ensure the security of the data?

How will personal or other sensitive data be handled to ensure safe data storage and transfer?

STANDARD: "Project data will be stored on file servers managed by USI IT service in folders with limited and managed access permissions. The principal investigator (applicant) will be in charge of deciding which researchers have access to the folders containing the data."

2.3. How will you handle copyright and Intellectual Property Rights issues?

Outline the owners of the copyright and Intellectual Property Right (IPR) of all data that will be collected and generated, including the licence(s). For consortia, an IPR ownership agreement might be necessary. You should comply with relevant funder, institutional, departmental or group policies on copyright or IPR. Furthermore, clarify what permissions are required should third-party data be reused. (This relates to the [FAIR Data Principles](#) I3 & R1.1)

Who will be the owner of the data?

STANDARD: USI is the owner of the data.

Which licenses will be applied to the data?

What restrictions apply to the reuse of third-party data?

See [§1.5.2](#).

3. Data storage and preservation

3.1. How will your data be stored and backed-up during the research?

Please mention what the needs are in terms of data storage and where the data will be stored. Please consider that data storage on laptops or hard drives for example, is risky. Storage through IT teams is safer. If external services are asked for, it is important that this does not conflict with the policy of each entity involved in the project, especially concerning the issue of sensitive data. Please specify your back-up procedure (frequency of updates, responsibilities, automatic/manual process, security measures, etc.).

What are your storage capacity and where will the data be stored?

What are the back-up procedures?

STANDARD: "The project data will be stored and processed on file servers managed by the IT service of USI, which are protected by backup copies of data (backup) made every night of the working days."

3.2. What is your data preservation plan?

Please specify which data will be retained, shared and archived after the completion of the project and the corresponding data selection procedure (e.g. long-term value, potential value for reuse, obligations to destroy some data, etc.). Please outline a long-term preservation plan for the datasets beyond the life-time of the project. In particular, comment on the choice of file formats and the use of community standards. (This relates to the [FAIR Data Principles](#) F2 & R1.3)

What procedures would be used to select data to be preserved?

What file formats will be used for preservation?

See [§1.4](#).

4. Data sharing and reuse

4.1. How and where will the data be shared?

Consider how and on which repository⁹ the data will be made available. The methods applied to data sharing will depend on several factors such as the type, size, complexity and sensitivity of data. Please also consider how the reuse of your data will be valued and acknowledged by other researchers. (This relates to the [FAIR Data Principles](#) F1, F3, F4, A1, A1.1, A1.2 & A2)

*On which repository do you plan to share your data?
How will potential users find out about your data?*

See [§1.6](#).

4.2. Are there any necessary limitations to protect sensitive data?

Data have to be shared as soon as possible, but at the latest at the time of publication of the respective scientific output. Restrictions may be only due to legal, ethical, copyright, confidentiality or other clauses. Consider whether a non-disclosure agreement would give sufficient protection for confidential data. This relates to the [FAIR Data Principles](#) A1 & R1.1)

Under which conditions will the data be made available (timing of data release, reason for delay if applicable)?

See [§1.5.1](#).

4.3. I will choose digital repositories that are conform to the FAIR Data Principles (Yes / No)

The SNSF requires that repositories are conform to the FAIR Data Principles. If there are no repositories complying with these requirements in your research field, please deposit a copy of your data on a generic platform. If no data can be shared, this is a statement of principles.

4.4. I will choose digital repositories maintained by a non-profit organization (Yes / No)

If the answer is no: "Explain why you cannot share your data on a non-commercial digital repository." The SNSF supports the use of non-commercial repositories for data sharing. Costs related to data upload are only covered for non-commercial repositories.

⁹ A list of generalist, discipline-specific and institutional data repositories commonly used by Swiss research community can be found [here](#)

Contacts

Research and Transfer Service
Università della Svizzera italiana
Via Buffi 13
6900 Lugano
Switzerland

e-mail igor.sarman@usi.ch

web <https://www.usi.ch/it/universita/info/srit>

© Università della Svizzera italiana