

Data Protection Review in research

The Data Protection Review Form highlights the key aspects that require careful planning and implementation when collecting and processing personal data in research projects.

If you wish to obtain support from the Data Protection Officers (DPOs) in assessing the legal compliance of your research data processing activities, please send them the completed Data Protection Review Form by email (dpo@unifr.ch). The review should be carried out before any personal data is collected or processed.

You can also refer to your ethics application if the same questions were addressed.

The Project		
Project title		
Brief description of the project and its intended aim		
Planned project duration		
Principal Investigator / Project manager	Name	
	Department/Institut	
	Email	
Ethics and Legal review of project by another body <i>Has another body already reviewed the project regarding the legal and/or ethical aspects of data collection and processing?</i>		
Collaboration <i>Indicate whether the project is conducted exclusively by UNIFR researchers or as a collaboration. If collaborative, specify the partner and their role. Specify if students are involved in the project and their role.</i>		

Data collection		
Source of personal data <i>How do you obtain this personal data?</i> <i>Examples: collection from participants, reuse of data collected in a previous project carried out at UNIFR, reuse of data transferred by another research institution, collection of data published on the web and social media, data published on an online research portal or repository (FAIR data), etc.</i>		
Research techniques, instruments and equipment <i>Specify all the research techniques you use to collect the data.</i>	Survey (please attach)	
	Individual interviews (please attach)	
	Interview/discussion in focus groups (detailed description)	
	Participant observation (detailed description)	
	Video/audio recordings (details of tools/equipment used, etc.)	
	Data from social media (please state which platforms and relevant consent from platform providers, etc.)	
	Combination of datasets (detailed description)	
	Others (detailed description)	
Sensitive personal data <i>Specify if you collect sensitive personal data and if so, which types.</i> <i>Sensitive personal data means:</i> - data relating to religious, philosophical, political or trade union-related views or activities; - data relating to health, the private sphere or affiliation to a race or ethnicity; - genetic data; biometric data that uniquely identifies a natural person; - data relating to administrative and criminal proceedings or sanctions; - data relating to social assistance measures. <i>Examples: fingerprints, medical images; hospital records; biological and genetic characteristics; membership in a political party or religious group; sexual orientation; criminal records, ...</i>		

Research project participants Specify whether : - a specific category of participants is concerned (e.g. Unifr students, pupils in compulsory education in the canton of Fribourg, ...) - the participants can be considered as a vulnerable group (e.g. children, people with disabilities, people in precarious situations, prisoners, people unable to give consent...), - there is a significant imbalance of power between the PI (and the research team members) and the participants, favouring the PI (e.g. participants are students in a lesson taught by the PI) ?	
Consent Specify if you research project participants consent to the collect and processing of their data. Please attach the information sheet and the consent form	

Data processing and data security		
Pseudonymisation / Anonymisation If you pseudonymise the data: specify how and what key management is used If you anonymise the data: specify how. Otherwise, specify why you need to use unanonymised data.		
Data security Specify the technical and organisational measures to ensure the confidentiality, availability and integrity of the data : infrastructure storage, access rights, back-ups, means of sharing data in the event of collaboration with people outside the Unifr, ...		
What happens to the data at the end of the project If the procedure varies depending on the dataset, please specify this for each one.	Data is stored in a repository for reuse (specify the repository, the de-identified process, the restrictions of access and reuse) Data is deleted Data is fully anonymised Data is archived on institutional infrastructure (specify the data security measures) Other (specify)	

Technologies	
Technologies used for the data collection and processing <u>Examples</u> : online surveys, data management tool, data storage tools, data analysis tools, transcription tools, mobile computing via smartphone apps, AI agents, ... For each technology, specify whether it is provided by a third-party service provider (Software as a Service, cloud hosting, ...) or whether it is on-premises infrastructure (Unifr institutional infrastructure) For each technology provided by a third-party service provider: - specify the data processed with the technology and its form (pseudonymised or not) - provide the relevant license agreement/legal terms/data privacy policy/data processing agreement... for each third-party service provider.	