**Guide on student collection of personal data**

This guide is for students who are collecting personal data for use in master’s theses, bachelor projects and other projects where you have described the purpose yourself. As a rule, you, as a student, need to ensure compliance with data protection rules, which is why the guide does not describe the situations where you work on existing research data or receive data from SDU.

**1. Introduction**

Before you start collecting personal data for use for projects, there are some things you need to consider. You need to assess whether you are dealing with personal data or anonymised data at all. If you use personal data, please be aware of compliance with the rules of the **General Data Protection Regulation** (GDPR). Anonymous data can be processed without taking GDPR into account.

You must have the consent of the participant to collect personal data. It is essential to describe the purpose of the data collection and allow participants to make up their minds about whether or not they wish to participate. In addition, you need to think about what types of information you need to use, for how long and how to store it, and whether it should be passed on for purposes other than your project, for example. It is essential that the formal things are in place **before** starting the collection of data. After you finish using the personal data, be sure to delete it.

**2. Data responsibility**When you need to use the personal data for your project, there are two places you can get data from – from the participants themselves or from someone other than the participant themselves. To make it easier for you, we split up the two situations as they are treated differently in terms of both practical and legal aspects. There is also a process diagram that describes the processes.

1. You decide how your project will be designed and which personal data you will use for the analyses. You are responsible for collecting the personal data directly from the participants. This means that you are responsible for ensuring that the rules of the GDPR are complied with and that data is generally in order. The SDU is not responsible for this type of tasks where the purpose is defined by yourself. It is still possible to get help and guidance, among other things, from IT about secure applications and storage solutions. It also means your master’s thesis should not be notified to SDU RIO.
2. If, on the other hand, you have been given a predefined project by your supervisor or are associated with an existing research project, that is another matter. This is the case if you do not collect the personal data yourself, but need access to data that has already been collected. Then, your supervisor should contact SDU RIO to ensure that all the rules are complied with so you can get lawful access to data.

**3. Personal data**

Personal data is any information that can be used to identify a person. Quotes, photos, video and audio recordings may also be personal data. This also applies even though the individual information must be linked to other information before it is possible to identify the person. Personal data is only anonymised when it is impossible to identify people based on the information.

A quote can also be a personal data: *‘I am the Queen of Denmark’.* This quote contains no name but it does contain

specific information about a particular office. It could be several different people, but with the date, it will be

possible to identify the person.

Thus, it is not enough to use a coding system in which a civil registration number is replaced by a code. As long as it is possible to backtrack the information using the code, the process is called pseudonymisation, and the information is still personal data. This applies even if only one person has the code for the information. You therefore need to be very aware of whether your information is personally identifiable and whether you have mastered the relevant security measures required by the GDPR. It is not certain that a piece of information is anonymous in a legal sense, even if you believe it is anonymised.

**5. Prior to collection**

Before you start collecting personal data for your project, you need to give some thought to the collection itself.

The collection must take place in a secure manner, and you must therefore explore the possibilities of using secure systems, have a plan

for how data should be stored, how you obtain consent, when deletion should take place etc.

It is an overarching principle of the GDPR that no more data may be processed than is necessary to fulfil the purpose. This means that you need to decide on what information you will need and thus not collect any information that is irrelevant. This is called data minimisation. During your analyses, you must also keep in mind that you may only store personal data you actually need.

**6. Consent**

You must make sure you have obtained valid consent from the person you want to collect information about – **before** you start collecting any data. This applies regardless of whether you need to record video, take pictures, have answers to a questionnaire or something completely different. There are four conditions that must be met before a consent is valid:

* + The consent must be *specific*, so that it is adapted specifically to the task and purpose that is relevant.
	+ It should be *voluntary*, so that there are no inconveniences associated with saying no.
	+ It must be *unambiguous*, so tacit/implied consents are not valid.
	+ Finally, it must be *informed*, so that the participant is informed of his or her rights.

A request for consent must be easily accessible, understandable and be in clear and plain language. Therefore, you should avoid using any specialist expressions, if possible. We recommend that you obtain written consent, as you must be able to prove that consent has been given – and what the participant has specifically consented to.

The participant may withdraw his or her consent at any time. If this happens, you are no longer allowed to process personal data and must therefore delete any data you have about the person.

Before giving consent, the participant must be informed that he/she/it may withdraw their consent. The process of withdrawing one’s consent must not be more cumbersome than providing it. If a declaration of consent has been made, it is a good idea to allow the participant to withdraw their consent by email or phone. The participant must have sufficient information about their rights and the specific circumstances in relation to the assignment and the processing of data. This is a prerequisite for the consent to be valid.

In the case of information about children, a specific assessment must be made on whether the child can consent. In such cases, it is decisive which personal data is involved and the maturity of the child must also be taken into account. It must be assessed whether the child can understand the consequences of consent and here the nature of the information is of great importance. In general, an ordinary 15-year-old is considered sufficiently mature to be able to consent himself. In the case of a particular group that, for example, has cognitive difficulties, it will require parental consent. If the child does not have the necessary maturity to consent, it is the custodian who must consent[[1]](#footnote-1). However, the child must still be informed about the project to the extent that it makes sense – given the child’s age etc.

SDU RIO has created a template for a consent statement that you are free to use.

**7. Duty of disclosure**

When obtaining consent, participants must be informed of their rights so that they can decide whether or not to consent. It is part of the condition that the consent must be informed. The participant must be informed of:

* + the identity and contact details of the data controller and his/her/its representative, if any;
	+ the purposes of the processing for which the personal data is to be used and the legal basis for the processing;
	+ any recipients or categories of recipients of the personal data;
	+ where processing is based on consent, the consentee must be informed of the right to withdraw their consent at any time; and
	+ the right to lodge a complaint with a supervisory authority (the Danish Data Protection Agency).

In addition, you can choose to disclose the items below (depending on the specific circumstances)

* + the period for which the personal data will be retained or, if that is not possible, the criteria used to determine that period,
	+ the right to request from the data controller:
		- * insight into the personal data processed about the participant,
			* to correct and adapt personal data that is not correct; or
			* to delete personal data; or
			* to restrict processing concerning the data subject; or
			* the right to object to processing.

If you use SDU RIO’s declaration of consent, the disclosure obligations are part of the template.

**8. Security**
There are various requirements for the handling and storage of personal data. This must be done in a reassuring manner – with an appropriate level of security and privacy protection. This means that, for example, you are not allowed to store personal data in your bag or in your Dropbox. Some systems are more secure than others. You can contact IT Services for help choosing a secure storage solution.

# Process diagram

1. If the parents are divorced but still have joint custody, it is the residential parent who must give consent. [↑](#footnote-ref-1)