How to manage personal data in your study projects

In the spring of 2018, the European General Data Protection Regulation (GDPR) came into force. Its purpose is to ensure a proper treatment of the personal data of EU citizens and prevent abuse.

All companies and institutions in the EU have to comply with this regulation. Also Business Academy Aarhus, who has implemented new guidelines and procedures to protect your personal data.

However, you also have a responsibility - as a student you are a representative of the institution. When you collect personal data, do surveys and gather other types of data in your study projects, you are the **responsible data processor**. It is important that you follow the regulation. The EU can hand out fines of up to 4% of the annual turnover of an institution. In theory it can be done on the basis of how you treat and protect personal data in your study projects.

What is personal data?
A distinction is made between common and sensitive personal data.

Common personal data	*Sensitive personal data*
- basic information e.g. name, gender, age, address, phone number, date of birth - information on education, references, exams, course certificates, employment, duties, grades - information on salary, tax, pension and bank account - sick leave - email address - social security number	- race or ethnic origin - political, religious or philosophical beliefs - union membership - health information including genetic data - biometric data for identification purposes - sexual relationships or orientation - criminal offences

Being the responsible data processor, you have to handle both the common and the sensitive personal data in accordance to the new General Data Protection Regulation.

Here is what the regulation means for you and your way of organizing research in your study projects:

Respondents must give consent
You can’t just throw an online survey out there and then scrape in all the personal data. All respondents must give a clear consent - and they must be informed of how they can withdraw this consent again.

What does a consent look like?
No formal template is able to fit all situations, so draw up your own document. According to the Danish Data Protection Agency an agreement must be "voluntary, specific and informed". This means that you have to describe exactly how you plan to use the personal data, so that the respondent knows, what he is agreeing to. For documentation purposes, the consent has to be in a written or electronic form.

You may base your document of consent on this structure:

Why are we asking for your consent?
What data are we asking for, and for what purpose will we use it?
How do you withdraw your consent?
What happens to your data when we finish processing it or you withdraw your consent?

How do you get the consent?
In an *online survey* you can start with a field where the respondent can tick off his consent. It must be an active action, and therefore a pre-filled field is not sufficient. It is also not sufficient to assume that the respondent automatically gives his consent by choosing to participate.

Also you need to state the nature of the consent and how it can be withdrawn. E.g. insert a link to a project blog where the information is permanently published and can be retrieved.

When doing *interviews* and *focus groups* you should draw up a physical consent form that people can sign. Give participants a copy, so they get to keep information about the consent and the process of withdrawal.

When respondents withdraw their consent
Everyone has the right to withdraw their consent at any time and you have to make sure that it is possible. In fact, the consent is invalid, if this is not in place. Respondents need to be able to find you again. Give out you contact information if you meet respondents in person. Or create a form or a single check box for withdrawal of the consent on a project blog.
When someone withdraws a consent, you have to stop storing and processing their personal information. In reality this means that you have to delete their data, e.g. by removing it from the data material you are analyzing.
You may however still use the results that came out of your data processing prior to the withdrawal.

You have to decide for yourself if you have time to adjust any calculations based on the original data, or if you have to include a note in your project report explaining that the pool of respondents got reduced during the project period.

What can you use the collected personal data for?
You can use the data for the specific purpose you collected it for - and got the consent for. Not for anything else. Often that means research or user tests in connection to a study project. You may not share the personal data with others, and when your task is done, you have to delete the data.

As a consequence, you cannot attach a survey with visible personal data as an appendix to a project, since it can be retrieved through the library. Instead, attach a resumé or an anonymous version.

Pictures and videos ALSO count for personal data
As a rule, you also need consent to publish pictures or videos of persons, whether it is online, in a project report or as a part of a developed product or concept. That applies for both portraits and situational motives where specific persons take part.
Only exception is if you take situational and decorative pictures where people are unidentifiable, e.g. of people in public situations, such as waiting passengers at a bus stop or random bypassers in a street.

Anonymous data collection
If your data collection is 100% anonymous, it is not covered by the General Data Protection Regulation. However, if you want to avoid the regulation completely, you cannot ask for contact information, in order to be able to contact specific persons again. If you do, it requires a consent.

Why all the fuss?!
It may seem unnecessarily difficult to comply with the General Data Protection Regulation. Definitely you will have to rethink your research and data collection process in order to follow the regulation. But try to see it as a general and much needed protection of all of us. When businesses and institutions are expected to guard your personal data, of course you have to show the same type of care when gaining access to other people’s personal data.

Read more about the General Data Protection Regulation (GDPR) from these sources:
The Danish Data Protection Agency (Links til en ekstern webside.)Links til en ekstern webside.
The European Union - EUR-Lex (Links til en ekstern webside.)Links til en ekstern webside.