Workshop: sharing personal data through a data repository, 28.11.2023

Questions and Answers

Researchers who work for a cantonal university apply cantonal laws. What about participation in an EU project - researchers have to conform to the GDPR, don't they?

Researchers must apply European law in the following cases:

- If they travel to a European country to collect data;
- If they work with European citizens or people living in Europe as part of their research design. For example, they want to know how German people work, how they vote, how they travel, etc. If researchers target European citizens or residents, even if the research is conducted in Switzerland, they have to apply the GDPR.

If researchers are collecting data in Switzerland from a European citizen, but are not interested in the fact that he or she is a European citizen, they don't need to apply the European law.

Today, we are used to having collaborative research projects with several universities, including universities in Europe, which fall under the GDPR. So when building a collaboration convention, you should have a contract that will make your project GDPR compliant.

If I am reusing data from a third party (e.g., an administration, schools, an NGO, a company…), am I responsible for making sure of the legal conformity of the original data collection process? Am I accountable for finding a legal basis, etc.?

You are not responsible for the legality of the initial data collection.

That said, gathering information from a third-party institution is also data collection. It is therefore subject to the same obligations as any other collection. For example: you must have a legal basis for the collection and inform individuals of this collection (unless they have already been informed, e.g. at the time of the initial collection).

In this kind of situation, the best way to go is to have a data transfer contract which clearly defines the responsibilities of each party. In this contract, the institution communicating the data may, for example, declare that it has done the data collection legally, that it is disclosing it legally, etc. Legal offices are quite used to drawing up this type of contract/convention.

If we use a client management database, and upon creation of a client, they automatically receive an email stating that we comply with data protection laws and that if they are satisfied with this, they have nothing to do, and if they are not happy with this they must reply and opt out, is this enough?

It depends on what kind of data you are collecting. If the data that you are collecting is sensitive data, opt out is not an acceptable solution. For the collection of sensitive data, consent must be explicit (and opt out is not an explicit consent). The best way to go in this case is to have a checkbox that allows people to actively consent.

Is there any recommendation about how to store and collect consent contracts? Aren't they sensitive personal data themselves, as they help to recognize who participates in the studies?

It is good practice to store consent contracts in a separate storage place and protect them with encryption and specific access rights. The best way is to let one person who is not part of the research team store them in an institutional location (e.g. private server).

Does the "basis of research privilege" work for the GDPR for all EU countries, or is it only in Swiss law?

Yes, there is a basis of research privilege for GDPR too. There are some specific provisions for research activities.

Here in the UK, informing participants about sharing data is considered as an ethical obligation so it cannot be archived unless participants have been informed of this.

It is the same for Switzerland. It is compulsory to inform participants of any disclosure to third parties and/or collection of data. People must therefore be informed that their data are (or will be) shared via a third-party repository and with which categories of recipients.

Is protection lost as soon as a person is deceased?

Yes. Data protection is what we call in Swiss law “a personality right”, and as sad as it is, personality ends with life. So once a person is dead, the data protection laws don't apply.

So, if pseudonymised data are archived at a repository without the key that enables identification, is this considered personal data?

It’s not an easy question because there are debates about this amongst lawyers. If the research falls under the scope of the Human Research Act, then the data remains personal even if it is coded and the user does not have access to the key. This is what is called the “absolute” perspective. From the General Data Protection perspective, things are more nuanced. Some legal experts say that the data are not considered as personal from the point of view of the researcher who gets the data and who does not have access to the key (relative vision), while others argue for the absolute vision. There is no definitive answer because there is no jurisprudence on that question for now.

What elements should we pay close attention to in a depositor contract, to make sure we are dealing with a trustworthy repository? I would not want to lose my rights over my dataset, for example, by depositing it, right?

All repositories have their own conditions, so it is important you look into them when choosing a repository. We would suggest you select in the first place a repository which complies with the FAIR data principles, as required by the SNSF. You can find the list here: www.re3data.org
As a depositor you should keep your rights over your dataset. This is certainly the case if you chose SWISSUbase as your data repository.

Is DataGo based upon Swiss laws or cantonal laws (and if cantonal, which canton)?

DataGo is based on Swiss law. It takes the more general perspective. It is normally compliant with all cantonal laws, since we tried to be as comprehensive as possible.

Who are the contact persons for DataGo?
Pablo Diaz (pabloandres.diaz@unil.ch) and Alexandra Stam (alexandra.stam@fors.unil.ch)

The tool itself is open source, right? Technically we could collaborate to deploy it on other local law regimes?

The code is open source, yes! It would be great to make it grow. We plan to develop it in the near future to make it relevant for researchers at the start of their projects (as opposed to researchers who have already collected their data, as is now the case).

In what sense is DataGo different from Papago?
The technology behind DataGo is the same than that of Papago, but the topic is different. Papago assists with Open Access, while DataGo assists with the sharing of research data through an archive.

Some links:

Link to Papago: https://www.unil.ch/openscience/en/home/menuinst/open-access/papago---your-open-access-personal-assistant.html
Another link shared during the workshop: a "fun" website to get a grasp of just how re-identifiable people can be based on a set of only a few personal data elements: https://www.ooa.world/