Managing Sensitive Data in the Era of Open Data

UZH Summer School, 25 August 2020

Pablo Diaz, Marieke Heers (FORS)

FORS

About ourselves…

Swiss Centre of Expertise in the Social Sciences

- Methodological research
- Large-scale surveys
- Data and research information services

Archiving services

FORSbase

Data management support

Training

Consultancy

Development of materials
(i.e. guides) **https://forscenter.ch/publications/fors-guides/**

Insights from the field…

«Who is in favour of Open Data?»

«Who applies Open Data?»

Different levels of resistance:

- Across disciplines
- Across methodologies
- Across cultures

FORS

Challenges to data sharing

- Subjective (habits, personal views, career)
- Practical (lack of know-how, discipline-specific guidance)
- Normative (charters, rights, legal obligations)

Challenges are especially important when it comes to sensitive data:

- Subjective: «sensitive data cannot be shared»
- Practical: lack of know how (data protection techniques)
- Normative: ‘contradictory’ forces between data openness and data protection laws

Managing sensitive data: a legal matter (?)

Sensitive data is a legal notion. The **Federal Act on Data Protection (FADP)** provides the following definitions:

Processing	Personal data	Sensitive data
Any operation with data, irrespective of the means applied and the procedure, and in particular the collection, storage, use, revision, disclosure, archiving or destruction of data. (Art. 3 lit. a FADP) The person who decides on the purpose and means of data processing is called the **data controller.**	All information relating to an identified person. (Art. 3 lit. a FADP) The person whose data is processed is called the **data subject.**	Personal data on: 1. Religious, ideological, political or trade-union; related views or activities 2. Health, the intimate sphere or the racial origin; 3. Social security measures; 4. Administrative or criminal proceedings and sanctions. (Art3. lit. c FADP)

FORS

Managing sensitive data: a legal matter (?)

- Sensitive data cannot be managed without knowledge of existing laws.

- The processing of this type of data is governed by a certain number of legal rules related to **data protection**.

- While data management is never a purely normative issue, the implementation of adequate strategies necessarily requires an understanding of the regulatory framework, in the sense that it provides the fundamental definitions, the limits not to be exceeded and the rights of each person (researchers and participants).

Data protection laws

Anyone who processes personal/sensitive data is subject to legal obligations.

In Switzerland there are laws at :

- The **federal** level (FADP)
- The **cantonal** level (LPrD, LCPD, etc.)

In Europe: there is a General Data Protection Regulation (GDPR).

On a world scale, 132 out of 194 countries had put in place legislation to secure the protection of data and privacy.

https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Which law(s) apply and when?

In order to determine which law(s) apply and when, the main criteria to be taken into account are:

- Place of **establishment** of the data controller (PI)
- **Legal status** of the data controller (private, federal, cantonal…)
- Geographical **location** of data collection (Switzerland, EU…)
- **Sector** of activity (health…)

These criteria are cumulative!

Establishment criterion

We are always subject to the laws of the country in which we are working.

- If you are working in Switzerland, you are subject to Swiss data protection laws (federal, cantonal, etc.).
- If you are working in Europe, you are subject to the GDPR.
- Etc.

This criterion is independent of the place of data collection and/or processing as well as the place of origin and/or establishment of the persons whose data are processed.

Legal status criterion

In Switzerland, the legal status of the data controller determines which law applies (federal or cantonal).

Private person/company	Federal body	Cantonal body
Federal laws apply	Federal laws apply •EPFL, ETH, FORS, etc.	Cantonal laws apply •UNIL, UNIGE, UNIBE, UNIZH, HES, etc.

If you carry out research as an employee of a university, you are subject to cantonal laws.

Geographic criterion

What matters here is where the participants are when the data are collected as well as the intention to target specific populations.

- If you **travel** to a country to collect data from people there, the laws of that country apply (whether or not the participants are residents).

- When **targeting** populations/individuals according to geographical criteria, the laws of the country where they are located apply, even if the collection and processing is carried out/organised from Switzerland (internet questionnaire, etc.).

Targeting does not need to be precise/explicit to be legally considered as such. If you create an online participatory platform and translate it into several languages (+ country selection), this can be considered targeting (intention).

Examples of (non) application of the GDPR

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The GDPR has extraterritoriality clauses. It is therefore (theoretically) applicable outside the EU.

- If a researcher from *UNIL* conducts an *ethnographic* investigation on the political behaviour of *French residents*, the **GDPR applies (+ LPrD)**
  - UNIL -> cantonal law Vaud (LPrD)
  - Targeting of French residents (GDPR)
  - Data collection in France (GDPR)

- If *FORS* organises an online questionnaire open to *all European citizens* (translated into all European languages), the **GDPR applies (+ FADP)**
  - FORS -> federal law (FADP)
  - Targeting of EU citizens -> GDPR

Examples of (non) application of the GDPR 2

- If a UNIBE researcher organizes a questionnaire to measure satisfaction with the supply of day-care centres in Switzerland, the **GDPR does not apply. The LCPD applies.**
  - UNIBE -> Cantonal law Bern (LCPD)
  - Targeting of Swiss residents -> GDPR does not apply (even if EU citizens)

- If an ETH researcher subcontracts the processing of certain personal/sensitive data to an institute based in Germany, the **GDPR applies to the subcontractor. The FADP applies to the researcher.**
  - ETH -> Federal law (FADP)
  - Subcontractor in the EU -> GDPR (establishment criterion)

Sectoral criterion

Certain sectors of activity are regulated by specific laws that take precedence over FADP in the matter of data protection.

Researchers working on diseases as well as on the structure and function of the human body have their activities regulated by the Human Research Act (HRA)

More precisely, if your research is on:

- The causes, prevention, diagnosis, treatment and epidemiology of impairments of physical and mental health in human beings
- Human anatomy, physiology and genetics, non-disease-related research concerning interventions and impacts on the human body, etc.

The HRA applies and **stricter data protection measures are required!**

Legal framework in Switzerland

In this workshop, we will focus mainly on the **Federal Act on Data Protection (FADP)**, as the cantonal laws are quite similar (although sometimes more flexible).

Warning: the FADP is currently being revised by the federal chambers in order to align it with the GDPR. There will be some important changes, but as far as we are concerned (research) the spirit remains the same. The entry into force of the new law is expected in early 2022.

The FADP

This Act aims to protect the privacy and the fundamental rights of persons when their data is processed (Art. 1 FADP)

Data protection is first and foremost about people, not data!

It is the persons whose data are processed that need to be protected, not the data themselves.

Nor does FADP seek to (legally) protect the data controller (e.g. with detailed/complicated consent forms, etc.)

*The FADP subjects data controllers to a number of duties when processing **personal/sensitive data**!*

The FADP 2

FADP makes informed consent **mandatory** for any processing of **personal data**.

If the data collected is **not sensitive**:

- Consent can be **oral**
- Consent can be **implicit**

If the data collected is **sensitive**:

- Consent can be **oral**
- Consent must be **given expressly**

The FADP 3

Within the framework of a research activity, the FADP allows the processing of personal/sensitive data **without informed consent**.

That said, **a number of conditions must be met**, among which (Art. 22):

- The data must be rendered **anonymous**, as soon as the purpose of the processing permits;
- The results must be published in such a manner that the data subjects **may not be identified**

*These conditions are **difficult** to meet…especially in the era of open data. For this reason, **consent** remains the best option.*

The GDPR and research (in brief)

Like the FADP, the GDPR provides for a number of derogations for scientific research activities, with the aim of facilitating the processing of personal data in this area.

That said, the researcher must always:

- Inform about any **collection** and **processing** (even anonymisation)
- Carry out a **Data Protection Impact Assessment** when the project is likely to involve “a high risk” to the privacy of individuals

The GDPR and consent

For the consent to be valid (i.e. informed), the data controller must provide the following information to the data subject:

- The identity and contact details of the data controller
- The contact details of the Data Protection Officer ;
- The purposes of the processing operation for which the personal data are intended and the legal basis of the processing operation;
- The legitimate interests pursued by the controller or by a third party ;
- The recipients or categories of recipients of the personal data,
- Where applicable, the fact that the controller intends to carry out a transfer of personal data to a third country or to an international organisation

The GDPR and DPIA

A Data Protection Impact Assessment (DPIA) is required under the GDPR any time you begin a new project that is likely to involve "a high risk" to the privacy of individuals.

Examples of the types of conditions that would require a DPIA:

- If you're using new technologies
- If you're tracking people's location or behavior
- If you're systematically monitoring a publicly accessible place on a large scale
- If you're processing sensitive data
- If your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects
- If you're processing children's data

From theory to practice…

- The processing of sensitive data is subject to compliance with the rules established by law. These rules depend on who you are, where you are and what you do.

- That said, whatever the applicable framework, three elements are essential:

  - Risk Assessment
  - Informed Consent
  - Anonymization

- To implement them it is not enough to know the rules. It is also necessary to develop a practical sense. This is what we will explore in the workshop

Thank you !

PabloAndres.DiazVenegas@unil.ch
Marieke.Heers@fors.unil.ch