Your driving licence in Data Protection

The purpose of these infographics is to provide the EPFL research community a resource to help it to manage correctly the personal data involved in their research projects, to protect the privacy of the data subjects and to ensure high data protection and scientific standards.
**The main definitions**

**Personal data** is all information relating to an identified or identifiable person. It is not so important what form personal data takes - it may be a sign, a writing, an image, a sound or a combination of these elements.

**Data subjects** - these are the natural or legal persons whose data is processed.

**Sensitive personal data** includes data on: (1) religious, ideological, political or trade union-related views or activities; (2) health, the intimate sphere or the racial origin; (3) genetic data; (4) biometric data which unequivocally identifies a natural person; (5) data on administrative or criminal proceedings and sanctions; (6) social security measures.

**Profiling** includes any form of automated processing of personal data consisting of using such data to assess certain personal aspects relating to a natural person.

→ For more information, you can consult Chapter 2: The main definitions in the guidelines.
The applicable legal framework

Swiss Federal Data Protection Act (FADP) - The main data protection law in Switzerland is the Federal Act on Data Protection (FADP), accompanied by the Ordinance to the Federal Act on Data Protection (FDPO).

EU-General Data Protection Regulation (EU-GDPR) - In an effort to update the protection of personal data in the European Union, the European Parliament has adopted the EU-General Data Protection Regulation (EU-GDPR) which entered into force in May 2018 in the European Union.

For more information, you can consult Chapter 4: The applicable legal framework in the guidelines.
When you collect data, you usually ask data subjects for consent. A comprehensive informed consent is a crucial requirement in research.

- The data controller must prove that consent has been given.
- The data subject has the right to withdraw consent at any time.
- Consent is not required where processing is authorised by a legal or contractual basis (except for compliance with the Federal Act on Research involving Human Beings).

Consent for Sensitive / Health related Data - For research falling under the responsible of Swissethics there are specific templates for consent available in website: https://www.swissethics.ch/en/templates/studieninformationen-und-einwilligungen

For more information, you can consult Chapter 5: Research Personal Data Life Cycle in the guidelines.

GDPR + FADP
- Right of access
- Rectification
- Opposition to processing
- Erasure
- Portability of data
Throughout the project, the security aspects must be taken into consideration. Researchers should be aware of IT security, which is one of the key principles of the Data Protection Act, and ensure they are trained in security.

**Awareness:**
Researchers should be aware of IT security, which is one of the key principles of the Data Protection Act, and ensure they are trained in security.

**Legal framework:**
Don’t forget internal LEX! LEX 6.1.3 et 6.1.4

**Pre-project**

**During the project**
- Define a security incident procedure
- Ensure your storage (y.c cold storage) is secure
- Ensure your back-up is in place
- Ensure that your servers / PC / tablets or other IT device are safe
- Traceability in place
- Users access rights

**In case of third party or sub-contractors,** define and put in place contractual / organizational / technical measures in order to secure your data.

**Ensure that**
- your servers / PC / tablets or other IT device are safe
- your back-up is in place
- traceability in place
- users access rights
- define and put in place contractual / organizational / technical measures in order to secure your data

**Throughout the project**
- Users access rights
- Traceability in place
- Ensure your back-up is in place
- Ensure your storage (y.c cold storage) is secure
- Ensure your servers / PC / tablets or other IT device are safe

**Remember your precious help...the IT Admin of your unit!**

→ For more information, you can consult Chapter 10: Appendix Security measures to implement in the guidelines.
Open Research Data (ORD) is research data that is publicly available for reuse, in an appropriate form and with minimal restrictions, e.g. permissive licenses. The principle of openness is not in contradiction to authorship or possible commercial exploitation of such data. The same applies to the presence of potentially personal data in ORD.

Plan for ORD
Invest the time in preparation and planning. When planning, explore various techniques to minimise the presence of personal data. Analyse your hypothesis and design of experiments. Define what is minimum needed data. Consider the level of detail needed for your research. If you cannot avoid personal data during collection, anonymize, when possible.

Avoid
Avoid collection of exact data, if possible. Lessen the collection of explicit data. Give preference to clustering, e.g. instead

Reduce
Reduce the amount of personal data to a minimum. Always check beforehand if the data that you wish to collect is necessary for your research. Ask control questions, such as “Do I need this information for my research?”.

Anonymize
When you anonymize data that you have created, you manage the anonymization process. However, when you receive data from a data provider, make sure that the data is anonymized. The best way to do that is to seek information on the anonymization process directly from the data provider.

Separate
Apply a fine-grained vision of your data - consider open/close not at the level of projects, or datasets, but when possible at the level of data fields. Split dataset into more parts, divide personal and not personal data.
At EPFL you have many entities that can provide you with support throughout the project. Most of the actors should be contacted in the initialization phase (plan) of your project, mainly the:

- Research Office (ReO)
- Library
- VPA Legal-DPO
- IT Admin - IT Security

Throughout the project, all EPFL support units are at your disposal in regard to personal data.

→ For more information, you can consult Chapter 3: The main stakeholders and EPFL support units in the guidelines
Health data belong to sensitive data and must be protected in an appropriate way.

The lack of an adequate protection entails significant legal, financial, reputational and scientific risks. For example, there can be criminal and civil sanctions if a research project that involves sensitive data processing is not compliant (for example no ethics authorization was obtained, a clinical trial requirement is not met and participants encounter a health problem).

IT and physical security measures to implement are described in the Appendix of the guidelines. They include security measures to protect personal data and some additional measures.

For more information, you can consult Chapter 6: Health Data Management in the guidelines.

SV-IT team can help you to implement such systems and provide the adequate support in case of need.

Different IT systems exist at EPFL that are compliant with the strict regulations on health data.