UNIFR OPEN SCIENCE WEEK
Open Data and Management of Sensitive Research Data
1. Data management involves many legal fields.

2. In the academic world, everybody has to manage different data.

3. These data, depending on the field of research and the partners involved, are often covered by confidentiality clauses, professional secrecy, functional privacy, data protection, patent law...

4. To understand the general legal context and to apply the organizational and technical measures key skills are needed.

5. The question is... what is your role and where to start?
COURSE OBJECTIVES
IDENTIFY THE MOST RELEVANT LEGAL QUESTION

YOU ARTISTS SHOULD BE GRATEFUL FOR US LAWYERS. WE PROTECT YOU!
FROM WHAT?

LAWYERS!
“Until now, data archiving platforms in the fields of humanities and social sciences in Switzerland mainly focused on technical issues of research data archiving. However, the introduction of the European General Data Protection Regulation (GDPR), the need to have complete Data Management Plans (DMPs) for projects of the Swiss National Science Foundation (SNF), and the upcoming revisions of the Swiss Federal Act on Data Protection (FADP) and the Swiss Federal Act on Copyrights and Related Rights (CopA), a good understanding of the legal background of data management becomes more and more important in order to reduce legal risks and avoid high penalties. However, often it is not easy for researchers to orient themselves within the legal jungle. It is therefore necessary to identify the most relevant legal questions and provide specific solution approaches that are easily understandable also to legal laymen.”

1. MANY LEGAL FIELDS

- Private law
- Contractual restrictions
- Public law
- Labour law
- Intellectual property
- Secrecy requirements
- Data protection
- Archiving, bookkeeping
- Regulatory requirements
- Criminal law
- Professional secrecy
- Functional privacy
1. MANY LEGAL FIELDS

CONTRACTUAL RESTRICTIONS

• Contracts
  • Research (with SME, industry)
  • Cloud (Open Science)

• Clauses
  • Confidential clauses
    • Protection of secrets (personal or material data are concerned, business secrets)
    • Intellectual property rights, know-how
    • Data collection (customer base)
    • Professional secrets (Medical, Bank clients)
  • Exclusivity clauses
  • Exclusions or limitation of liability clauses
1. MANY LEGAL FIELDS

- Private law
- Contractual restrictions
- Public law
- Labour law
- Intellectual property
- Secrecy requirements
- Data protection
- Archiving, bookkeeping
- Regulatory requirements
- Criminal law
- Professional secrecy
- Functional privacy
1. MANY LEGAL FIELDS
INTELLECTUAL PROPERTY

- Copyright
  - Co-author, authentification, conflict management
- Trademark
- Patent
  - Protection of secrets (technological innovation, condition of novelty)
  - Research and cookies
  - Communication and security

“One of the rationales for patents is that they stimulate economic and technological development and promote competition by creating a financial motivation for invention in return for the disclosure of the invention to the public. Although the potential of the patent system has been widely recognized in the context of dynamic innovation activities, some critics have claimed that the current patent system stymies R&D and technological advances.”

1. MANY LEGAL FIELDS

- Private law
- Contractual restrictions
- Public law
- Labour law
- Intellectual property
- Secrecy requirements
- Data protection
- Archiving, bookkeeping
- Regulatory requirements
- Criminal law
- Professional secrecy
- Functional privacy
1. MANY LEGAL FIELDS
DATA PROTECTION

• General principles applicable to the processing of personal data

• These principles should be considered as an introductive guideline and basic framework for the particular requirements for processing personal data

  • Lawfulness, fairness and transparency
  • Purpose limitation
  • Data minimization
  • Accuracy
  • Storage limitation
  • Integrity & confidentiality
• Processing data in a transparent manner to the data subject means not only providing the relevant information of the processing activity itself, but also informing the data subject in regards to their data subject rights

• “Emphasise that transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of their personal data, which could serve as a basis for improved information requirements.” (European Commission, Commission staff working paper, Impact Assessment, 25.01.2012)

• Fundamental right
• Difficult but possible: AI & Transparency
First component:
- Collect for specified (sufficiently defined, depending on the particular context and prior to the collection)
- explicit (sufficiently unambiguous and clearly expressed and should leave no doubt or difficulty in understanding)
- and legitimate purposes (in accordance with the law in the broadest sense, legitimacy of a given purpose can also change over time)

Second component:
Not further processed in a manner that is incompatible with those purposes
- Requires a compatibility test (double negation prohibiting incompatibility - means, any further processing is still authorised as long as it is not incompatible)
1. MANY LEGAL FIELDS

MINIMALISATION

- Personal data shall be “adequate, relevant and limited to what is necessary”
- No universal approach of determining the necessity of the data processing activity
- Has to be assessed in relation to the specified, explicit and legitimate purpose for which the data have been collected on a case-by-case basis
- Think about the option: Anonymisation! Closely linked to the principle of purpose limitation
1. MANY LEGAL FIELDS
NECESSITY

• Factual Element: Personal related data shall only be processed if and to the extent that such processing actually casually supports the fulfilment of the relevant purpose
• Judgmental Element: Personal related data shall only be processed if and to the extent that the relevant purpose cannot be reasonably achieved by other means avoiding such processing
1. MANY LEGAL FIELDS

- Private law
- Contractual restrictions
- Public law
- Labour law
- Intellectual property
- Secrecy requirements
- Data protection
- Archiving, bookkeeping
- Regulatory requirements
- Criminal law
- Professional secrecy
- Functional privacy
Dual-use items can be used for both civilian and military applications. Switzerland controls the export, transit and brokering of dual-use items to contribute to international peace and security and prevent the proliferation of Weapons of Mass Destruction (WMD).

- Export Controls are rules and restrictions imposed by governments (based on international agreements as mentioned earlier) on businesses on the movements and transfers of activities related to certain listed
  - goods,
  - software and
  - Technology

- In scope of the Dual use regulation is: the export, the import, the transit and the brokerage of above mentioned items
1. MANY LEGAL FIELDS
REGULATORY REQUIREMENTS

• Technology & Dual Use
  • Means information for the development, manufacture or use of goods that is neither generally accessible nor serves for purposes of pure scientific research (e.g. software, access to software and technology – such clouds computing etc.). This information takes the form of Technical data or technical assistance.

**Basic Principles of Export Controls**
Principles in Academia

- Sensitive subject matters:
  - Biology, including Biotechnology and Medicine
  - Chemistry, Biochemistry
  - Physics
  - Nuclear Technology
  - Energy and environmental technology
  - Information and communication technology
  - Electrical Engineering
  - Aerospace and transport technology
  - Mechanical Engineering
  - Materials Engineering- Process Engineering
2. DIFFERENT DATA
GENERAL – PERSONAL - SENSITIVE

General Data Protection Regulation (GDPR)

All Data

Personal Data
Requirements:
1. notice of privacy
2. explanation for use of Personal Data
3. consent to use/transfer the data outside of EEA

Examples:
- name and surname
- home address
- email address
- ID card number
- IP address
- cookie ID
- phone identifier
- data held by a hospital or doctor that could be used to identify a person

Special Categories of Data
Requirements:
1. explanation of the need for this sensitive data
2. explanation that the US may not offer the same protection of personal data
3. explicit consent to use and/or transfer that type of data

- racial/ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for identifying a person
- health-related data
- sex life or sexual orientation

https://research.ucr.edu/ori/faq/faq-gdpr
2. DIFFERENT DATA

SENSITIVE DATA

• Personal data revealing racial or ethnic origin, political opinions, religious and philosophical beliefs [...] health or data concerning a natural person’s sex life or sexual orientation

• Processing data must be justified by the data subject’s explicit consent
2. DIFFERENT DATA

CLOUD ISSUES

- Data security
- Data process in by third parties
- Cross-border transfer
3. FIELD OF RESEARCH

PARTIES INVOLVED

• COMPLEX – CASE: Research with big Pharma – exclusivity - to be published – where?

• COMPLEX – CASE: Research with a watchmaking company – check the novelty - check the plagiarism – when – to publish?

• COMPLEX – CASE: Arbitrage court ou big pharma requires personal data in the companies?
4. TOMS
DATA PROTECTION

Data breach due to:
• Lack of confidentiality
• Availability
• Integrity

• Security regulations (appropriate technical and organizational measures TOMs)

• Sanctions EU EUR 20 million / 4% annual turnover – Sanctions Suisse CHF 250’000
4. TOMS
EX. ISO

- Foreword
- Introduction
- Scope
- Normative references
- Terms and definitions
- Structure of this standard
- Bibliography

8. Asset management
9. Access control
12. Operations security

5. Information security policies

6. Organization of information security

7. Human resources security

8. Asset management

9. Access control

10. Cryptography

11. Physical and environmental security

13. Communications security

14. Systems acquisition, development and maintenance

15. Supplier relationships

16. Information security incident management

17. Information security aspects of business continuity management

18. Compliance
# 4. TOMS

## ORGANISATION (UNIBAS)

<table>
<thead>
<tr>
<th>Klasse 0</th>
<th>Öffentliche Informationen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diese Informationen sind für die Öffentlichkeit bestimmt und können uneingeschränkt veröffentlicht und geteilt werden.</td>
<td></td>
</tr>
</tbody>
</table>

### Klasse I Interne Informationen

<table>
<thead>
<tr>
<th>Klasse II Vertrauliche Informationen</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diese Informationen sind für den universitätsinternen Gebrauch und nicht für die Öffentlichkeit bestimmt. Das Veröffentlichen oder die Weitergabe dieser Informationen hätte aber keine oder nur geringe negative Auswirkungen für die Universität oder einzelne Personen.</td>
</tr>
</tbody>
</table>

### Klasse III Geheime Informationen

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Diese Informationen sind aufgrund gesetzlicher oder vertraglicher Geheimhaltungspflichten nur für autorisierte Personen (Geheimnisträger) bestimmt. Das Zugänglichmachen an unberechtigte (universitätsinterne sowie -externe) Personen konnte negative Auswirkungen für die Universität oder einzelne Personen haben.</td>
</tr>
</tbody>
</table>

*inkl. gewöhnlich Personendaten*

*inkl. besondere Personendaten*
5. YOUR ROLE
YOU HAVE TO ASSUME

YOU CAN'T BE TOO CAREFUL!
ACTUALLY YOU CAN BE TOO CAREFUL.
How can I protect myself from this new threat?!
5. YOUR ROLE

STOP THINKING

• We see the security as overvalued
• We are not an attractive subject for attack
• We have never been affected
• We have our systems under control
• We regulate ad hoc
• We have our techies
• We delegate the security
• We cannot afford it
• We are insured
• We are powerless
MORE ABOUT LEGAL STANDARDS

I MUST HAVE MORE KNOWLEDGE! MORE!!

WHY NOT USE THE KNOWLEDGE YOU ALREADY HAVE?

I SAID KNOWLEDGE, NOT WISDOM.
“How can I meet ethical and legal standards while respecting the epistemological and methodological codes of my discipline? How to respond to the growing demand for data openness without violating the new data protection rules? How do I store my data securely? Can I share everything? What will happen to my data after I retire?”


https://www.path2integrity.eu/ri-materials


https://www.pwc.ch/de/insights/regulierung/veraenderung-revidiertes-dsg.html
La fin de la publication scientifique ? Une analyse entre légitimité, prédation et automatisation
https://hal.archives-ouvertes.fr/hal-03435153
EXCURSUS
(SOURCE: ZÜRCHER VERWALTUNGSRATSKONFERENZ 2021)

Environment (E)
- Climate
- Water
- Other environment topics

Social (S)
- Health
- Employees
- Other social topics

Governance (G)
- Good governance
- Ethical standards
- Cyber security

Governance
- Overall accountability
- Roles and delegations
- Management oversight and interventions
- Incentives for Senior Management
- Assurance levels

Process
- Workflow and process management
- Lines of defense controls model
- Documented process and controls manuals
- Continuous improvement mindset and innovation approach

Managing ESG performance

Data
- Data definitions (users and producers to have the same understanding of the)
- Data collection (understanding the data lifecycle and knowing the origins)
- Data quality management processes
- Data governance

Systems
- Robust systems approach
- IT controls
- Integration of source systems to systems of record
- End to end automation