GDPR in general

- **EU General Data Protection Regulation (2016/679)**
  - Applied from **May 25th 2018** onwards
    - Supplemented by the Finnish Data Protection Act (1050/2018)
      - in force from January 1st 2019
  - The purpose of the new legislation is to improve and harmonize the rules of protection of personal data. The Regulation protects the fundamental rights and freedoms of natural persons, in particular with respect to the right to protection of personal data.
  - Accountability and evaluation of risks are key aspects of the new legislation
    - Compliance with obligations must be demonstrated with sufficient documentation
GDPR and TAU

• Research data at TAU often contains personal data;
• Data-intensive operating environment of the University requires that data protection principles are observed in all processing activities, including research.
• University Data Protection Policy (intranet)
• Other intranet data protection pages (coming very soon)

• Will you be processing personal data in your research?
Basic concepts and definitions – Personal data

- **Personal data**: means *any information* by which an individual (the “data subject”) is identified or may be identified either *directly* or *indirectly*:

- Usually identified correctly as personal data:
  - name,
  - social security number or other identification number,
  - address (incl. e-mail address)

- However, the concept of personal data is more expansive and also covers i.a.:
  - Title (All data when it can be linked with a certain person by using in combination with other items of collected data or even easily obtainable external data; tax law professor at TAU; only one exists now)
  - Video, photo, voice
  - Age, sex, place of birth, nationality, mother tongue, languages spoken, ethnical background…
  - IP address, location tags
  - Favourite colour, favourite ice hockey team
  - Answers to questionnaires (even with names removed), if the individual may be identified by a combination of factors specific to that individual (e.g. occupational/organizational status).
  - Anything you can connect/link to a person (interviews, observations, opinions, videos/photos of landscape or buildings etc.; i.e. also with no people in them)
Basic concepts and definitions – Personal data

- **Pseudonymized personal data**: the personal data can no longer be attributed to a specific data subject *without the use of additional information*, provided that such additional information is kept separately
  - for example: names of data subjects replaced with random codes; pseudonymization key kept separately
  - nb. pseudonymized personal data *is still personal data* and subject to data protection legislation
- **Anonymized personal data**: *All identifiers* have been removed in a way that *a person cannot be identified* from / on the basis of the data even when using additional information
  - Note: it is generally advisable to avoid claiming in your DMP and/or research plan that *you only process anonymous data*; anonymization, in terms of the GDPR, generally only applies to aggregated statistical data, provided that i) the sample size is large enough and ii) data is generalized and presented in rough groupings (which again, may have value as a research result, but not as the object of analysis)
  - Note that removing names from a data set is not anonymization, if the information can still be linked to an individual directly with other information or even indirectly with easily accessible additional information
    - removal of direct identifiers usually makes data pseudonymized data, not anonymized
    - normally some data must be reclassified when anonymizing it (in one class minimum 5, usually 10 datasets)
Basic concepts and definitions – Processing

- **Processing**: processing under the GDPR covers all actions relating to collection, use and storage of personal data
  - any operation or set of operations which is performed on personal data or on sets of personal data, *whether or not by automated means*, i.a.
    - collection, recording,
    - organisation, structuring, adaptation, alteration, combination
    - storage,
    - use, disclosure, dissemination
    - erasure or destruction.

- **Will you be processing personal data in your research?**
Basic concepts and definitions – Roles

- **Controller** means the natural or legal person, public authority, agency or other body which, *alone or jointly with others*, determines the purposes and means of the processing of personal data;
  - Determines what is done, why it’s done and how it’s done

- **Joint controller**: two or more parties determine the purposes and means together
  - Joint actions, consortiums if data is truly processed jointly

- **Processor** means the natural or legal person, public authority, agency or other body which processes personal data *on behalf of the controller* (i.e. a “subcontractor”)
  - Abides by the Controller’s orders (in theory..)

In University research, the university is typically the controller (alone or with other research organizations)
  - University employee is doing research, research funding is awarded to the university

Sometimes university is a processor (another organisation is controller, customer funded research)
  - Data storage even in situations where researcher/student is controller if data is stored in university network

Students are usually controllers in their own research for Bachelor’s/Master’s degree or PhD thesis.
  - Exception (rare cases): integrated/essential part of the university research project (same data set)
Principles of processing (Art. 5)

- Lawfulness, fairness, transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
Lawful bases of processing

- Processing of personal data is only allowed if the processing has a lawful basis as established in data protection legislation:
  - Art. 6:
    - Consent
    - Contract
    - Compliance with a legal obligation
    - Vital interests of the data subject
    - Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
    - Legitimate interests pursued by the data controller

- Bases of processing of special categories of data ("sensitive data") are stipulated in Art. 9 of the GDPR.
Applicable lawful bases in research

- Consent (Art. 6.1.a)
  - Consent for the research intervention ≠ consent as the basis for processing personal data
  - Using consent as the lawful basis may hinder the researcher’s ability to perform the research tasks as intended, and therefore it is generally advisable to use another basis for processing
    - Withdrawal of consent -> does not affect the validity of activities prior to withdrawal, but data may not be used for further analysis, validation purposes etc.
    - Right to data portability?
- => **Performance of a task carried out in the public interest** (Art. 6.1.e)
  - Status of scientific research as a "task carried out in the public interest" was affirmed in the national Data Protection Act
- Legitimate interests (Art. 6.1.f)
Principles of processing

- The scope and applicability of the principles must be evaluated on a case-by-case basis already when you are planning activities that involve the processing of personal data (e.g. in a research project) Careful planning will prevent problems later on.

- Risks must be assessed from data subjects’ perspective.

- Compliance must be demonstrated -> the importance of proper documentation

- Privacy by design and Privacy by default (Art. 25)
  - Privacy by design calls for privacy to be taken into account throughout the whole engineering process. The concept is an example of value sensitive design, i.e., to take human values into account in a well-defined manner throughout the whole process and may have been derived from this.
  - Privacy by Default means that once a product or service has been released to the public, the strictest privacy settings should apply by default, without any manual input from the end user. ... If more information than necessary to provide the service is disclosed, then "privacy by default" has been breached.

- Data processing plan is incorporated into the Data Management Plan and/or the research plan.
Principles in practice?

• When planning (and processing), consider at least the following questions:
  
  • 1. Do I need to collect personal data?
  • 2. Why is personal data collected and for what (lawful) purpose(s)?
  • 3. What is the minimum amount of personal data that I need?
  • 4. How do I collect the data?
      • Do I need to ask for consent? How do I inform the subjects?
  • 5. How do I store and maintain the data securely?
  • 6. How long do I need to store personal data (in an identifiable form)?
  • 7. How and when do I destroy or archive the data?
Principles in practice?

- Collect only if necessary
- Minimise
- Use for specified purpose(s) only
- Handle with care – do not leave paper documents lying on a desk. Store them in a locked cabinet. For electronic data, save data on a network drive with limited access or locally on a crypted harddrive.
- Never reveal personal data to others – personal data may only be processed by authorized employees as part of their duties.
- Transfer data securely – make sure that you are sending data to the correct recipient and encrypt data, if necessary.
- Report possible breaches and any suspicious activity.
Data Protection and Life Cycle of Research Project

- Pre-award phase (Research Funding Proposal)
  - Research plan
  - DMP
- Research funding awarded
- Post-award phase
  - Updated research plan
  - Updated DMP
  - Data protection documents
- Data collection starts
- Data analysis
- Possible updates of documents
- Etc.
Data Protection: Basic documentation

- In addition to DMP and research plan:
  - Obligation to inform the data subject
    - Privacy notice (Arts. 12—14)
      - Basic information concerning the processing activities in a project
  - Internal information
    - Record of processing activities (Art. 30)
    - Risk assessment
      - Risk based approach (always) (Art. 24)
    - Data protection impact assessment (Art. 35)
    - High risk -> Prior consultation of the supervisory authority (Art. 36)
  - Agreements relating to data processing
    - Joint controller agreements (if necessary), data processing agreements ("DPA" -> with external providers), material transfer agreements ("MTA")
"Treat the personal data of others as you would like your personal data to be treated"
Questions, comments?