Data protection in joint projects

Jukka Tuomela, data protection officer

Olli Repo, legal counsel

Anna Rytivaara, data protection specialist

Content

1. Data protection in research
2. Agreements on data protection in joint projects
   - Roles and responsibilities of processors
   - Agreements
     - Data processing agreement (DPA)
     - Joint controller agreement
     - Transfer agreements
3. Transfers outside EEA

Data protection in research

Data protection in research

- Data protection is the process of protecting personal data.
- Purpose of data protection: **why** and **how** personal data shall be processed
- Key questions:
  - Are personal data being processed?
  - What is the purpose of data processing=
  - Who is processing personal data?

Data protection in the university

- Data protection is a fundamental right and safeguards the rights and freedoms of data subjects (=research participants) when their personal data is processed.
- Data processing laws set out the principles for the lawful processing of personal data.
- The processing of personal data must always be based on law.
- Implementing data protection is a duty of all members of the university
- Responsibilities, principles and operating models confirmed in the data protection policy
- Instructions and document templates on data protection webpage

Data protection legislation in a nutshell

- EU's General Data Protection Regulation (GDPR)
  - To be applied in all EU/EEA countries
  - In some parts has flexibility for national derogations
- Data Protection Act (1050/2018)
  - National derogations in Finland
  - Definition of "public interest"
    - Scientific and historical research
    - Data archiving
- Act on the Openness of Government Activities (621/1999) "Openness Act"
  - Permission to access documents, also classified documents and registers
- Act on the Secondary Use of Health and Social Data (552/2019)
  - Use of personal health and social data for secondary purposes, such as scientific research

Principles of processing personal data

When processing personal data, the following principles are to be applied:

- Lawfulness, fairness and transparency
- Purpose limitation (”collected for specified, explicit and legitimate purposes”)
- Data minimisation (”adequate, relevant and limited to what is necessary”)
- Accuracy
- Storage limitation (processing period)
- Integrity and confidentiality (access to data, data security)
- Obligation to demonstrate that the principles are being applied

More detailed desciptions: https://www.tuni.fi/research-data-protection

To what purpose is personal data processed?

- Data shall be collected for **specified**, **explicit** and **legitimate** purposes and not further processed in a manner that is incompatible with those purposes; lawful basis defined in GDPR
- The purpose of processing determines the lawful basis
- In general, the lawful basis in university research: “processing is necessary for the performance of a task carried out in the **public interest;** “scientific or historical research” defined as such a task
  - N.B. Lawful basis not “consent” – different from consent to participate in a study

Definitions: processing personal data (GDPR, article 4)

- *Processing* means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as
    - collection,
    - recording,
    - organisation,
    - structuring,
    - storage,
    - adaptation or alteration,
    - retrieval,
    - consultation,
    - use,
    - disclosure by transmission, dissemination or otherwise making available,
    - alignment or combination,
    - restriction, erasure or destruction;

Data protection documentation

- **Planning the processing activities:**
  - Instruction: data protection path in research
  - Instruction/template: data protection checklist
  - Research data services; research services (DMP, H2020 Ethics, research plan)
- **Applying the principles and risk assessment regarding the processing:**
  - Template: concise risk assessment (Art 32)
  - Template: Data processing impact assessment (DPIA) (Art 32 and 35)
    - Instructions included in the template
  - Instructions: Risk assessment
  - Instructions: Prior consultation of supervisory authority (Art 36)

tuni.fi/en/research-data-protection

Data protection documentation (part 2)

- **Informing the research participants (data subjects)**
  - Template: Privacy notice for research: (Art 12—14)
  - Template: Information sheet
  - Template: Consent form (research ethics)
  - Instruction: Privacy notice for research
- **Data processing agreements**
  - Data processing agreement (Art 28)
  - Joint data controller agreement (Art 26)
- **Thesis research**
  - Template: Privacy notice for thesis (Art 12—14)
  - Instructions for thesis students concerning data protection
  - Instructions for supervisors concerning data protection

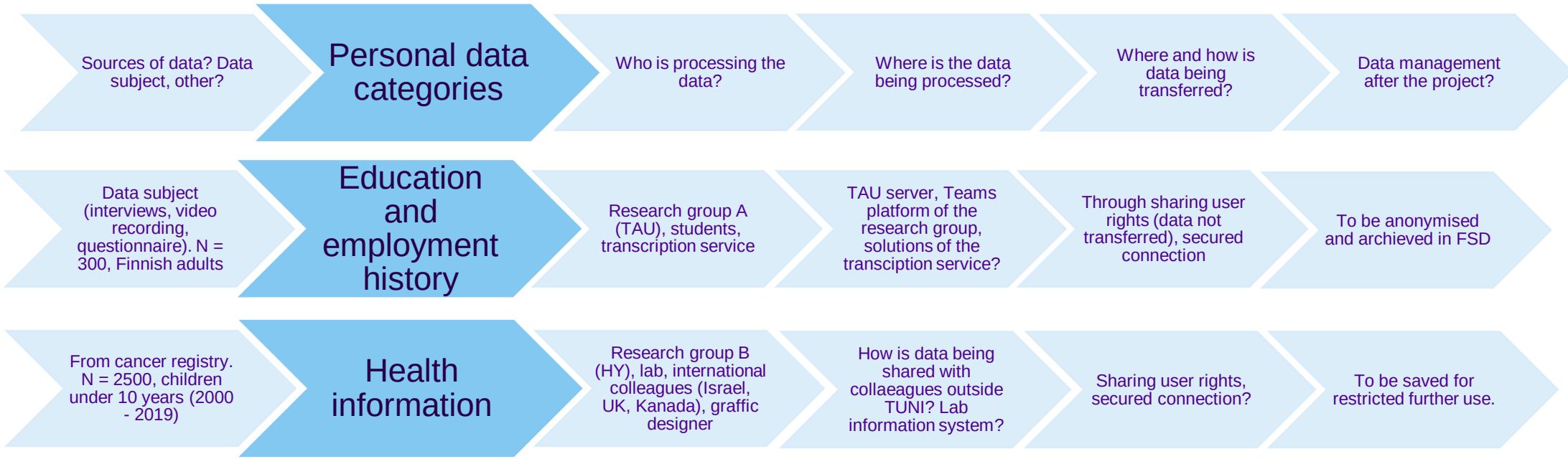
tuni.fi/en/research-data-protection

Data protection agreements in joint projects

Who is processing personal data?

- Are there more than one party planning the project?
  - What are the roles of each party in processing the data?
  - Are all data being collected from the data subjects or also from other sources?
  - Does the researcher/data controller handle all the processing activities or are services bought (data platforms, transcription)?
- Drafting a data flow chart is voluntary
  - Information about the parties, their roles and data flow helps enormously both the researchers and the support services

Data flow in research (examples)



Roles: data controller(s)

- Data controller:
  - determines the purposes and means of the processing of personal data
  - natural or legal person, public authority, agency or other body
  - In university projects usually the university
- Joint controllers:
  - At least two controllers determining the purposes and means of the processing of personal data
  - Frequent in national or international consortiums or joint projects, in which the parties decide together the purposes and means of the personal data
- ”Controllers in common”
  - At least two controllers processing the same data but each determining independently the purposes and means of the processing of personal data

Roles: responsibilities of the controller

- Controller has the overall responsibility of the obligations of the data protection legislation
- Controller is responsible for the lawfulness of the processing
  - In their own action and
  - When using external service providers, also committing the service providers in lawful processing, inclusing sub-contractors
- University as the data controller/processor is responsible for
  - Training and instructing their staff (GDPR art 29)
  - Instructing the external service providers

Roles: processor

- Processing personal data for and behalf of the controller
  - Sub-study from an external service provider
  - Internet-based data platforms
  - Survey and analysis services
  - Other support services, e.g. transcription, translation
  - Researchers outside TUNI, theses researchers
- Natural or legal person, public authority, agency or other body
- In university projects, usually the service provider

When agreement is needed?

- “Where processing is to be carried out on behalf of a controller” (Art 28)
  → Written processing agreements required
- ” Where two or more controllers jointly determine the purposes and means of processing"
  - In case of a joint registry (Art 26), mutual responsibilities to be determined **in a transparent manner**
  - → either a joint controller agreement, joint data privacy notice or other?
- N.B. separate agreement often required, for example,
  - Data disclosure
  - Providing data access
  - Archieving the data

Types of agreements

- **Data Processing Agreement**, DPA
  - Outsourcing processing activities controller → controller
- **Joint Controller Agreement,** JCA
  - Joint processing controller & controller
- **Data**/Material **Transfer Agreement**
  - Data disclosure controller → controller

→ If the roles and responsibilities of the parties are clear (research plan, DMP), drafting an agreement only requires documentation of the agreed modes of action

- Support services only support; careful planning and suffiecient backgroun information essential

(Data Processing Agreement, DPA)

Data Processing Agreement (28 article)

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

(a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

(b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all measures required pursuant to Article 32;

(d) respects the conditions referred to in paragraphs 2 and 4 for engaging another processor;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

(f) assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.

Data Processing Agreement (28 article)

- Take-aways:
  - Processing ”shall be governed by a contract or other legal act”
  - The contract needs to include:
    - the subject-matter and duration of the processing,
    - the nature and purpose of the processing,
    - the type of personal data and categories of data subjects and
    - the obligations and rights of the controller
  - ”Shall stipulate, in particular”:
    - documented instructions
    - statutory obligation of confidentiality
    - security measures required pursuant to Art 32
    - Role of sub-processors
    - obligation to respond to requests for exercising the data subject's rights
    - Impact assessment, prior consultation of supervisory authority
    - Data breach incidents
    - audits
    - Obligation to provide the controller with information regarding the processing
    - Return or destruction of the data at the end of the agreement

Data Processing Agreement (28 article)

- In practise:
  1. Data processing agreement (DPA)
     - => Obligation to agree, nature and scope of processing, parties' responsibilities
  2. Documented instructions of the data controller
     - => Information security and data protection requirements
       - In procurement (information security -excel) and functional requirements
       - In research, general desription of safety measures, often as an attachment of the agreement
       - N.B. "all personal data is processed in accordance with GDPR" is not sufficient
- DPA template
  - PI/researcher fills in the yellow-marked sections (Purpose of processing, processing activities, personal data categories)

Joint Controller Agreement, JCA

Joint controller agreement (26 artikla)

Article 26

Joint controllers

1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects. The essence of the arrangement shall be made available to the data subject.

3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

Joint controller agreement JCA (Art 26)

- Take-aways:
  - Responsibilities ”shall be determined **in a transparent manner**”, particularly:
    - Process data subject’s requests
    - Provision of information to the data subjects (art 13-14)
    - Data subjects can be provided with a single contact point
  - Other:
    - Scope, duration, purpose, personal data types, groups of data subjects
    - Division of costs (data management, joint procurements)
    - In research projects:
      - Risk assessment → DPIA → prior consultation of supervisory authority (who will handle)
      - Information security (in transfer, at rest..)
      - Actions after processing is finished?
    - Exchange of information in case of e.g. data breaches
    - Liabilities (art. 82)? Data subject may address their claims to either one
    - Essence of the agreement shall be made available to the data subject
    - Usually the essential parts are described in the privacy notice

Joint controller agreement JCA (Art 26)

- No legal obligation to draft an agreement (cf. DPA)
  - Possible to agree on the roles and responsibilities in a privacy notice
  - Often makes privacy notice hard-to-read → separate JCA preferred
- JCA template
- Project managers shall fill in:
  - Description of the purpose and aims of the processing (on a general level)
  - Nature and extent of the processing (or reference to the privacy notice)
  - Roles in i)impact assessment, ii)obligation to inform the data subjects and iii)exercise of the data subjects' rights; either naming a coordinator or each on their behalf; obligation to assisnt
  - Information security measures in collecting, storing and transferring the data
  - Dta processing after the project

Data/Material Transfer Agreement

Transfer or disclosure of data to external parties

- Personal data will be regularly transferred or disclosed to parties other than the members of the research group when, for example:
  - Data is transferred to another research group for analysis
  - An external processor is transcribing interviews or entering data in a statistical analysis software.
- What is the difference between transfer and disclosure of data?
  - Transfer occurs e.g. within a consortium, consortium maintains the responsibility over processing
  - In disclosure, responsibility over processing personal data is transferred to the recipient, and the **data controlled is changed**

Transfer agreement

- Data transfer agreement (DTA) concerns data
  - Databases, spss-data, excel-sheets
- Material transfer agreement (MTA) concerns material
  - E.g. samples (blood or cell samples)

Transfer agreements

- **Disclosure is a processing activity**
    - Purpose, lawful basis, data protection principles
    - Who is disclosing data to whom and to what purpose?
        - **Disclosure needs to have a right for disclosure**
            - Informing the data subjects – how about further use of data?
            - Principle of specified purpose; N.B. research degoration
                - further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
        - **Recipient needs to have a right for processing the data**
        - Possible safeguards
            - Anonymisation/pseudonymisation
            - Diminishes the risks on both sides

Transfer agreements

- In case of controller-controller, need for an agreement at all?
  - Both parties responsible for processing on their own behalf
  - Documentation of the transfer/disclore is essential
- Data transfer agreement (e.g. spss-data, databases, excel sheets) may include restrictions or conditions similar to material transfer agreement (transfer of data material such as blood samples)
  - Assessment according to the general agreement policy of TUNI legal services

Data transfer outside EEA

Data transfers outside EEA

- Data transfers outside EEA require safety guards (V section)

Article 44

General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

- E.g. transferring personal data to a coordinator or funding body outside EEA (N.B. access = transfer); use of a processor located outside EEA; cloud-based data services

Data transfers outside EEA

- In a nutshell:
  - Processing needs to be lawful in EEA and
  - Basis for transfer a mechanism from V section

- Priority of the transfer mechanisms:

Data transfers outside EEA

- Appropriate safeguards
  - i) Transfer on the basis of EC's adequacy decision (Art 45)
    - Adequacy decisions
      - E.g. japan, Israel, Canada (with restrictions); UK in process
      - → treated as transfers within EU
  - ii) Transfer using appropriate safeguards (Art 46) in lack of adequacy decision
    - In practice, University has applied standard contractual clauses (SCCs)
      - No changes to be made if these are used
  - iii) Derogations for specific situations (Art 49)
    - E.g. consent, when the data subjects have been informed about the risks
      - N.B. This is an expection → consent shall not be used in case of frequent or extensive transfers

Data transfers outside EEA

- In practice:
  - **Virtual desk, if possible (contact researchdata@tuni.fi)**
    - Prior information: KPMG about to audit TAU virtual desk → Secure environment as mentioned in Law of secundary use of data (552/2019)
  - Other cases:
    - **Pseudonymise** (key only in TAU, not in service provider or recipient)
    - **Encrypt** (encrypted storage and delivery)
    - **Secure** (Ask recipient, incl. service provider, about their practices)

Thank you.
Questions, comments?

researchdata@tuni.fi