HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

CONTENTS

1. What is the GDPR
2. Processing of personal data – What does it mean?
3. Requirements for processing personal data
4. Risk assessment and safety measures
5. Transfer of personal data
6. The rights of data subjects

WHAT IS THE GDPR?

- General Data Protection Regulation
- Applied from 25 May 2018, repeals the Data Protection Directive and national laws based on the Directive
- Similar but less detailed laws on personal data have been in effect before the GDPR
- Applies whenever the University processes personal data regardless of the nationality of the people whose data is processed

WHAT IS THE GDPR?

- Aims to ensure a consistent level of privacy protection for natural persons throughout the EU + enable free movement of data in the single market
- Leaves some discretion to the Member States
  - Important for universities: Exceptions regarding scientific research
- The Finnish Data Protection Act entered into force on 1 January 2019
  - Supplements the GDPR and includes certain exceptions regarding research

DEFINITIONS

- **Data protection** (tietosuoja, dataskydd)
  - Part of fundamental privacy rights
  - Concerns the processing of personal data
- **Data security** (tietoturva, datasäkerhet)
  - Protects confidentiality, access and integrity of all data

PROCESSING OF PERSONAL DATA

PERSONAL DATA

- **Personal data** (henkilötiedot, personuppgifter) means any information relating to an **identified** or **identifiable**, living natural person (a **data subject** / rekisteröity, en registrerad).

PROCESSING

- GDPR: **Processing** (käsittely, behandling) 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**.
  - In other words, almost anything you can do to personal data, including merely storing it.

DATA CONTROLLER

- Rekisterinpitäjä/personuppgiftsansvarig
- Definition:
  - The natural or legal person, public authority, agency or other body
  - Alone or jointly with others (joint controllers)
  - Determines the purposes and means of processing
- In most cases, the controller is the university, not the researcher(s) or other personnel
- Responsible for meeting the requirements of the GDPR
  - However, as a representative of the university, the researcher must comply with the law and the university's instructions when conducting research
- Responsible for sanctions for failure to meet obligations

DATA PROCESSOR

- Käsittelijä/personuppgiftsbiträde
- A data processor processes personal data on behalf of a data controller
- Usually a contractor such as an IT service provider, translation/transcription company, company providing analysis services etc.
- No independent purpose for processing, processes on behalf of the controller
- A data processing agreement (DPA) is required between the controller and the processor

IN MORE DETAIL: PERSONAL DATA

- **Personal data** (henkilötiedot, personuppgifter) means any information relating to an **identified** or **identifiable**, living natural person (a **data subject**, rekisteröity/en registrerad).
- Identifiable: Directly or indirectly
- Identifiers: name, identification number, location data, online identifier, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This includes a person's face, voice etc.
- Once a person is identified or identifiable, any information relating to them is also personal data.

EXAMPLES: PERSONAL DATA

- Survey results
- Person A's answers:
  - Female
  - Age: 30–40
  - Lives in Helsinki
  - Likes pizza

EXAMPLES: PERSONAL DATA

- Survey results
- Person A's answers:
  - Female
  - Age: 30–40
  - Lives in Helsinki
  - Likes pizza
- It is not possible to identify the respondent based on the answers – the above information is not personal data.

EXAMPLES: PERSONAL DATA

- Person B's answers:
  - Name: Sample McSamplesson
  - Email: sample.mcsamplesson@fictionalemail.com
  - Age 45
  - Lives in Sampleston (a village with 50 residents)
  - Likes pizza

EXAMPLES: PERSONAL DATA

- Person B's answers:
  - Name: Sample McSamplesson
  - Email: sample.mcsamplesson@fictionalemail.com
  - Age 45
  - Lives in Sampleston (a village with 50 residents)
  - Likes pizza
- It is definitely possible to identify the respondent – All of the above is personal data.

EXAMPLES: PERSONAL DATA

- Person C's answers:
  - Male
  - Age 45
  - Lives in Sampleston (a village with 50 residents)
  - Likes pizza

EXAMPLES: PERSONAL DATA

- Person C's answers:
  - Male
  - Age 45
  - Lives in Sampleston (a village with 50 residents)
  - Likes pizza
- All of the information should be considered as personal data, as the respondent is likely *identifiable.*
- The situation would be different if C had not included his hometown or if he lived in a larger city.

ANONYMISATION AND PSEUDONYMISATION

- Pseudonymised data
  - Data from which direct identifiers have been removed
  - Still personal data and should be treated as such
  - Pseudonymisation is just one protection measure for personal data
  - In the USA, de-identified data means pseudonymized data
- Anonymised data
  - Data from which the data subject is no longer identifiable, identifiers have been permanently removed
  - Not personal data anymore (GDPR does not apply)

PERSONAL DATA OR NOT?

- Data held by other parties must be taken account when assessing whether certain data is personal data or not.
- ”account should be taken of **all the means reasonably likely to be used**, such as singling out, **either by the controller or by another person** to identify the natural person directly or indirectly”
- For example, car license plates: The owner of the car cannot be determined by simply looking at the license plate, but authorities have the necessary information → The license plate number is personal data.

REQUIREMENTS FOR PROCESSING

PRINCIPLES

- Lawfulness, fairness and transparency
- Purpose limitation: Data must be collected for a specific purpose, processing incompatible with the purpose is prohibited
- Data minimisation: Only necessary data may be processed
- Accuracy
- Storage limitation: Data should not be stored in an identifiable form for longer than necessary
- Integrity and confidentiality
- Accountability: Controller must be able to demonstrate compliance

PRINCIPLES IN PRACTICE

- Before collecting any data, define the purposes for which the data is used.
  - In some situations, the same data may be processed for multiple purposes.
- Only collect data that is necessary for the purposes of your research/teaching.
- Delete personal data when you no longer require it (i.e., contact details of research participants if there is no need to contact them).
- Assess the risks inherent in your processing and apply appropriate safeguards.
- Document the processing (see next slide)
- Take the rights of data subjects into account.

ACCOUNTABILITY: RECORD OF PROCESSING

- Under the GDPR, the data controller must maintain a document (record of processing activities) that includes the following information:
  - Data controller and data protection officer
  - Purposes of processing
  - Description of the categories of data subjects and categories of personal data
  - The groups to which personal data have been or will be disclosed
  - Information on the transfer of personal data to countries outside the EU/EEA or international organisations
  - Data storage times
  - Description of technical and organizational measures
- Meant for internal use but must sometimes be provided to the Data Protection Ombudsman
- It's possible to draft a separate record or to include the required information in a data management plan or data protection notice
  - Send the completed document to tietosuoja@helsinki.fi for archiving purposes

LAWFULNESS OF PROCESSING

- Processing personal data without lawful grounds is prohibited.
- Once the purpose of processing has been defined, the legal basis must be determined.
- Full list in Article 6 of the GDPR

LEGAL BASIS FOR PROCESSING

Legal bases for processing in scientific research

- In many cases, the legal basis is ”processing is necessary for the performance of a task carried out in the public interest” (Art. 6(1)(e) of the GDPR).
  - No consent needed for processing, but the data subject must be informed about the processing
  - Requirements: appropriate project plan, person/group responsible for research, data is only processed for research purposes
  - Please note that medical research may require consent in accordance with the Medical Research Act
- In some cases, the legal basis is ”the data subject has given consent to the processing of his or her personal data” (Art. 6(1)(a) of the GDPR).
  - E.g. commercial research not carried out in the public interest

LEGAL BASIS FOR PROCESSING

Other bases that may be relevant:

- Processing is necessary for the performance of a contract to which the data subject is party
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party
  - E.g., contact details of customers and suppliers

SENSITIVE PERSONAL DATA

- **Includes:**
  - Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership
  - Genetic data
  - Biometric data for the purpose of uniquely identifying a natural person
  - Data concerning health
  - Data concerning a natural person's sex life or sexual orientation
  - Criminal convictions and offences or related security measures
- May only be processed on specific grounds: However, processing is permitted for scientific research or fulfillment of legal obligations, or with the data subject's consent.
- Do not collect unless necessary for the purposes of processing!
- Requires particular care regarding safety measures.

CONSENT AS A BASIS FOR PROCESSING

- Definition:
  - any **freely given**, **specific**, **informed** and **unambiguous** indication of the data subject's wishes
  - by a **statement** or by a **clear affirmative action**
  - signifies agreement to the processing of personal data
- The controller must be able to prove that consent has been given
- Can be withdrawn
- Gives broader rights to data subjects than other bases for processing
- In addition to a single study, it is also possible to provide consent to certain *areas* of scientific research.

RISK ASSESSMENT AND SAFETY MEASURES

RISK ASSESSMENT

- Assess the risks inherent in your processing and implement security measures accordingly for the entire duration of the processing.
- It is the controller's duty to assess:
  - the freedoms and rights that may be endangered by the processing, and
  - the harm that the planned processing of personal data may cause.

DATA PROTECTION IMPACT ASSESSMENT

- Must be carried out before the beginning of the processing if processing is likely to result in a high risk to the rights and freedoms of data subjects.
- See: list of situations in the data protection guide for researchers or the Data Protection Ombudsman's website (https://tietosuoja.fi/en/impact-assessments)
- Check the list in the planning phase of the project, preferably every time the research involves processing of personal data. Signs to be especially aware of:
  - Large-scale processing of criminal convictions or offences or sensitive personal data
  - Processing of biometric data for the purpose of identifying an individual, genetic data or location data
  - Making exceptions to the obligation to inform data subjects
  - Processing of sensitive data when exceptions to data subject rights are made
  - Processing of data of vulnerable individuals
  - Combining of data sets in a way that is unexpected from the perspective of data subjects

DATA PROTECTION IMPACT ASSESSMENT

- If an impact assessment is necessary in your project, or if you are not sure whether it is necessary or not, contact the legal team (tutkimuksenjuristit@helsinki.fi) as soon as possible. The reseach lawyers will assist you with the impact assessment.
- The impact assessment must be carried out before the beginning of the processes, and provided to the Office of the Data Protection Ombudsman in certain cases.

DATA SECURITY

Heathrow Airport Limited fined £120,000 for serious failings in its data protection practices

Date **08 October 2018**
Type **News**

Heathrow Airport Limited (HAL) has been fined £120,000 by the Information Commissioner's Office (ICO) for failing to ensure that the personal data held on its network was properly secured.

On 16 October 2017 a member of the public found a USB memory stick, which had been lost by a HAL employee. The stick, which contained 76 folders and over 1,000 files was not encrypted or password protected.

The member of the public viewed the material it contained at a local library.

Although the amount of personal and sensitive personal data held on the stick comprised a small amount of the total files, of particular concern was a training video which exposed ten individuals' details including names, dates of birth, passport numbers, and the details of up to 50 HAL aviation security personnel.

The stick was passed to a national newspaper which took copies of the data before giving the stick back to HAL.

DATA SECURITY

- Almost always necessary: password protection on hard drives, access control/locks for physical documents
- Never store personal data on unencrypted USB drives!
- Personal data should be processed in pseudonymised format if identifiers are not required for the research
- Encryption, other additional measures for high-risk processing
- Never process personal data on the free consumer versions of cloud services (Google Drive/Docs, Dropbox etc.) or survey services (Google Forms, Surveymonkey etc.)
- Use locked secure bins for disposing of documents containing personal data
- More information: Data Support (for data management), information security team

TRANSFERS OF PERSONAL DATA

PROVIDING PERSONAL DATA TO THIRD PARTIES

- **Type 1** – Providing personal data to another data controller
  - E.g. in research collaboration
  - Any necessary limitations regarding the use of the personal data must be transmitted to the recipient along with the data
  - Collaboration agreement, data/material transfer agreement etc.
- **Type 2** – Providing personal data to a data processor
  - Outsourced services such as IT services, translation, transcription, analysis of samples
  - A data processing agreement is required, content mandated by the GDPR

SAFEGUARDS FOR INTERNATIONAL TRANSFERS

- Personal data cannot be transferred/disclosed to recipients located outside the EEA without special safeguards
- 1. Adequacy decision: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay
- 2. Privacy Shield (United States)
- 3. Standard Contractual Clauses
- 4. Informed consent of the data subject
- 5. Binding Corporate Rules

- Contact the legal team before providing personal data to third parties.
- The legal team will assist you with assessment of the situation, necessary agreements and safeguards, as well as any other legal questions related to the case.
- Research questions: tutkimuksenjuristit@helsinki.fi
- Teaching-related questions: lakipalvelu-opetus@helsinki.fi
- Other questions: tietosuoja@helsinki.fi

THE RIGHTS OF DATA SUBJECTS

THE RIGHTS OF DATA SUBJECTS

- This presentation includes a rough outline. More detailed information can be found on the Data Protection Ombudsman's website: https://tietosuoja.fi/en/rights-of-the-data-subject
- Not all data subject rights can be excercised in all situations. Some rights are related to a specific legal basis of processing. Please see: https://tietosuoja.fi/en/what-rights-do-data-subjects-have-in-different-situations

RIGHT TO BE INFORMED

- Old law: Rekisteriseloste/registerbeskrivning – No longer required, no need to send descriptions to the data protection authority.
- Instead: The information listed in Article 13 or 14 of the GDPR must be provided to the data subjects.
  - If the data are collected from the data subject, the information listed in Article 13 must be provided to the data subject at the time when the data are obtained.

Article 13

Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

(e) the recipients or categories of recipients of the personal data, if any;

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

3. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

4. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information.

RIGHT TO BE INFORMED

- University's one size fits all solution: data protection notice
- Available in Yammer's data protection group: https://www.yammer.com/helsinki.fi/#/groups/13861941/files
- The template is a tool for ensuring that all necessary information is provided to research participants. Using it is not mandatory if you can communicate the information in some other way.
- You may tailor the template to your own needs (as long as all necessary information is included)
- Practical example: The data protection notice seemed too technical for informing students and their guardians about a study conducted at schools. A letter describing the study in an easily understandable way was provided to the students and guardians. An URL leading to the data protection notice was included in the letter.

RIGHT TO BE INFORMED

- Exception: Informing is not mandatory if the data has not been collected from the data subjects themselves, and informing would be impossible or would involve disproportionate effort.
  - Possible reasons: the identity of the data subject is unknown, the source of data (example: research on messages posted on online message boards) or considerably large number of data subjects.
  - If this is the case, consider uploading the data protection notice on the website of the study if there is one.
  - An impact assessment may be necessary. Please contact tutkimuksenjuristit@helsinki.fi

RIGHT OF ACCESS

- Data subjects have a right to know:
  - Whether their personal data is processed
  - If yes, what data about them is processed (including copies of the data, preferably in electronic format)
  - Certain other information listed in Article 15(1) of the GDPR: this should already be in the data protection notice.

OTHER RIGHTS

- **Right to rectification** – The right to have incorrect or incomplete personal data rectified
- **Right to erasure** (right to be forgotten) – When one of the following applies:
  - the personal data are no longer necessary for the purpose for which they were collected
  - data subject withdraws consent
  - the data subject objects to the processing (right to object) and the objection has valid grounds
  - the personal data have been unlawfully processed
  - legal obligation/collected in relation to the offer of information society services

OTHER RIGHTS

- **Right to restriction of processing** – Usually temporary measure to assess whether the processing of personal data has been legitimate and can be continued (for example, if the data subject has used their right to object)
- **Data portability** – Right to have data transferred to another data controller
- **Right to object** – Right to contest processing in the public interest/legitimate interest. The controller must re-assess whether the processing is necessary, and stop processing or demonstrate that there are grounds for processing.
- **Right to object to automated individual decision-making**

EXCEPTIONS FROM THE RIGHTS OF DATA SUBJECTS

There are certain cases when the rights of the data subjects cannot be fulfilled, e.g.:

1. Fulfilling the request would prevent or seriously impair the purpose of processing (scientific research)
2. The request cannot be connected to the processed data due to anonymisation, pseudonymisation or other reasons
   - Do not collect additional personal data to re-identify data in order to respond to data subject requests, unless the data subject provides the data
3. The identity of the requesting party cannot be confirmed or the request is likely fraudulent

- The situation must be assessed on a case by case basis.

FULFILLING THE RIGHTS OF DATA SUBJECTS

- Before commencing your research, assess whether fulfilling the rights of data subjects would prevent or seriously impair the research. A data protection impact assessment may be necessary. However, the decision to make exceptions to data subject rights following a data subject request must always be made on a case by case basis.
- If you receive a data subject request and you are not sure what to do:
  - Data subject requests must be handled within 30 days, so contact the legal services as soon as possible.
  - University lawyers will help you assess the legitimacy of the request and what information should be provided or deleted.

MORE INFORMATION

http://www.tietosuoja.fi – Data Protection Ombudsman's website

https://flamma.helsinki.fi/en/HY375934 – Data protection guide for researchers

https://flamma.helsinki.fi/en/HY373909 – FAQ: Protection of study-related data

https://www.yammer.com/helsinki.fi/#/groups/13861941/ – Yammer data protection group

https://datasupport.helsinki.fi/ – Data support

https://flamma.helsinki.fi/fi/HY034212 – Information security instructions

Questions on data protection in research:
tutkimuksenjuristit@helsinki.fi

Questions on teaching matters:
lakipalvelu-opintoasiat@helsinki.fi

Other data protection questions:
tietosuoja@helsinki.fi