DATA PROTECTION

RDM ADVANCED 2023
ETHICAL AND LEGAL COMPLIANCE

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

WHAT IS THE GOAL BEHIND DATA PROTECTION REGULATION?

- Right to privacy and data protection is a fundamental right.
- Data Protection Regulation sets the possibilities for when and under what conditions data about individuals can be processed in an ethical manner.
- The goal behind data protection is to:
  - Protect personal data from unauthorized and inappropriate processing
  - Ensure the implementation of the rights and freedoms of data subjects

WHAT IS PERSONAL DATA?

- Name
- Adress
- Opinion
- IP-Adress
- Picture
- Location
- Feature
- Behaviour
- And so on…

Any information that can be connected to an individual.

SPECIAL CATEGORIES OF PERSONAL DATA

- Also called as ”sensitive data”
- As defined in the regulation:
  - Data concerning individuals' health
  - Racial or ethnic origin
  - Political opinions
  - Religious or philosophical beliefs
  - Genetic data
  - Biometric data when it is processed for the purpose of uniquely identify a person
  - Data concerning the persons sexual life or sexual orientation
  - Data relating to criminal convictioncs and offences
  - Trade union membership

It is allowed to process special category data in research, but the data must be secured more carefully.

UNDIRECT IDENTIFICATION, PSEUDONYMISATION AND ANONYMISATION

Undirect identification

- Data can be personal data even though you are not processing direct identifiers such as name or social security number if individuals can be identified from the data by other means
- E.g., information about persons rare disease or feature. Or if you are collecting lot of data from an individual so that the identity can be concluded

Pseudonymized data

- **Pseudonymized information is still personal data!**
- Direct identifiers (such as names) are removed or replaced with other identifiers (like number code)
- It is still possible to restore the data to be identifiable

Anonymized data

- Data is anonymous if it is not possible by reasonable means to connect the information to an individual
- Total anonymization is often quite challenging, which leads to situations that the data can often still be pseudonymous data aka personal data.

WHO IS WHO IN DATA PROTECTION REGULATION?

Controller, Joint controller, Processor?

WHY IS IT IMPORTANT TO UNDERSTAND AND DETERMINE THE ROLES IN PERSONAL DATA PROCESSING?

- The roles define who is responsible for ensuring that the requirements are implemented, and data subject rights ensured
  - This also in practice defines, which organizations guidance and compliance practices need to be followed
- Definition of the roles also gives a basis for the definition of rights and requirements for each party in the project
- The roles and responsibilities of the parties need to be informed also to data subjects

ROLES IDENTIFIED IN THE REGULATION

Controller is the one who is responsible for the legal compliance and possible damages to data subjects.

Contract (DPA)

Processor
Analyses, stores, destroys or by other means processes personal data on behalf of the controller.

Contract

Joint controllers:
Two or more organizations and/or persons determine the purposes and means for the processing together

WHO IS A CONTROLLER – UNIVERSITY OR THE RESEARCHER / STUDENT?

University of Helsinki is the controller for the research when

- the research is performed under an employment relationship with UH
- the research project is approved by the University and/or the funding for the research is allocated to the University (”UH’s research project”)

University of Helsinki is a joint controller with the researcher when

- Researcher/student is not in employment relationship with UH or is not performing the research as part of UH’s research project
- E.g., doctoral dissertations (without employment relationship), master theses

GENERAL PRINCIPLES

GENERAL PRINCIPLES

Lawfulness, fairness and transparency

- Process personal data only when you have a legal mandate to do so e.g. and usually: Research carried out in public interest (specific situations also consent)
- Be fair towards the research participants and other examinees, do not cause unnecessary risks
- Be open about the processing of personal data

Purpose limitation

- Use the data only for purposes it was collected and in a manner that was informed to data subjects
- Data can be used for future research projects if the purpose for processing is ”compatible” with the information that was given to the data subjects and/or if the possible data/research permit allows

Data minimisation

- Collect only the data you need for the research
- Erase all data you don’t need anymore
- Pseudonymize or anonymize the data when possible!

GENERAL PRINCIPLES

Accuracy	• Processed personal data should be accurate and kept up to date where necessary
Storage limitation	• Store personal data for as long it is needed • Personal data can be stored for future research purposes also (be transparent towards the data subjects and comply with other general principles)
Integrity and confidentiality	• Protect the data adequately, towards unauthorized access, destruction or damage

ACCOUNTABILITY

- Accountability means that you should be able to demonstrate that you comply with the regulation.
- In research this can be done by the help of the following documents/tasks:
  - Research plan
  - Data management plan
  - Data Protection Impact assessment (especially when required by law)
  - Data protection statement and possible consent forms
  - Agreements with partners
  - Possible research/data permits and ethical reviews

And of course, by taking the aforesaid into account and implementing the plans in practise!

RISK ASSESMENT AND DATA PROTECTION IMPACT ASSESMENT

How to avoid risks?

RISKBASED APPROACH

- implement appropriate (technical and organisational) measures to
  - implement data-protection principles in an effective manner and
  - integrate the necessary safeguards into the processing

- Take into account
  - Latest technology and the cost of implementation
  - The nature, scope, context and purposes of processing
  - The risks for rights and freedoms of natural persons

When you are planning your research, think of the risks to data subjects and plan how to mitigate them.

Define also how you will implement the general principles.

POSSIBLE RISKS & IMPACTS TO DATA SUBJECTS

For example:

- Fraud
- Negative impact to employment
- Sosial damage/damage to reputation, embarrassment
- Nuisance
- Verbal abuse
- Feeling of insecurity
- Inability to exercise rights
- Loss of freedom of political/religious opinions or beliefs
- Discrimination
- Bodily harm
- Loss of freedom of movement
- Loss of control over the purposes of processing of his/her personal data

POSSIBLE MITIGATION ACTIONS, MEASURES TO PROTECT THE DATA

- Safeguards can be, f. ex:
  - Data minimisation
  - Pseudonymisation, anonymisation
  - Encryption
  - Aggregation
  - Using encrypted email/connection when sending sensitive data
  - Contracts with partners
  - Instructions for persons processing the data
  - Defining access rights
  - Using secure processing environments
  - And so on…

WHEN DO YOU NEED TO PERFORM DATA PROTECTION IMPACT ASSESSMENT (DPIA)?

- The Regulation requires that a data protection impact assessment is performed and documented at least in situations where the processing of personal data *is likely to result* in a high risk to the rights and freedoms of data subjects:

  ➡ The risks and possible impacts need to be analysed in more detail

- UH have a template/checklist you can use to assess the need for DPIA. ”Does my research need a data protection impact assesment”-template (Link to: Flamma)
- In the pre-assessment you assess f.ex.: the scale of the processing, data subjects position, processed data and the means of processing

Do the preliminary assesment to evaluate whether the processing of personal data is regarded to cause a high risk to data subjects.

DATA PROTECTION IMPACT ASSESMENT (DPIA) – WHAT IS IT? (YOU CAN FIND THE TEMPLATE FROM FLAMMA)

- The idea is to identify and analyze the risks that the processing of the personal data causes to data subjects

- Helps you to manage the risks to data subjects plus possible compliance risks

- In practice:
  - The processing of personal data is described
  - Compliance check
  - The risks are identified and analyzed
  - Needed measures to mitigate the risks are defined

- The main point is to analyze and argument (plus document) whether the processing is acceptable in the first-place aka does not cause too high risks to data subjects

TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

- The goal behind the regulation in this context is to provide the same level of data protection like we have in the EU.

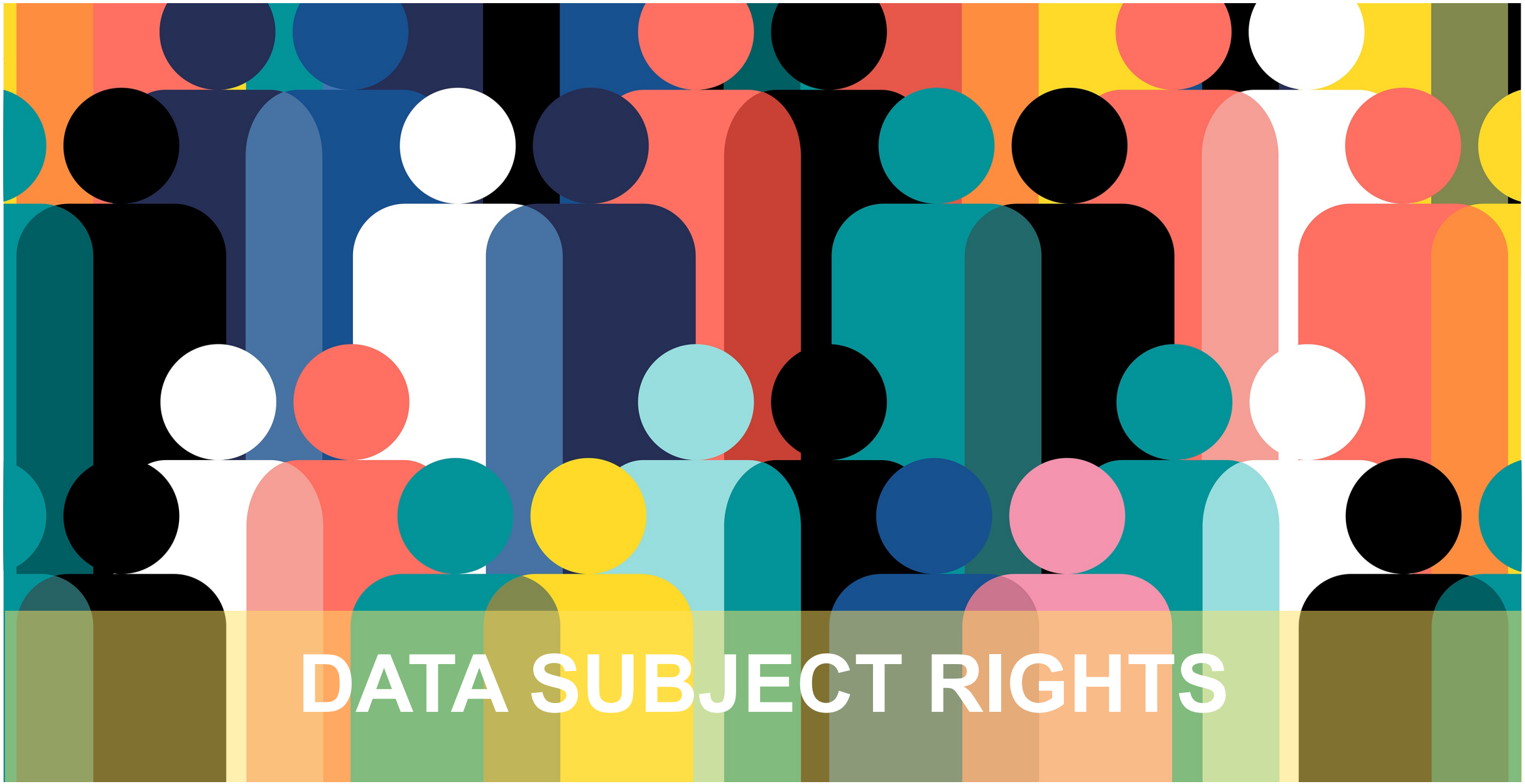
- When disclosing/transferring data outside the EU or granting access to data, attention must be paid to whether an adequate level of data protection has been established in the country of destination.
  - If not, extra transfer mechanisms and safeguards need to be used to protect the data and data subjects

TRANSFER OF PERSONAL DATA OUTSIDE THE EUROPEAN ECONOMIC AREA

- You can transfer/disclose data if EU Commission have declared that the country provides adequate level of protection (listed on Commissions websites): https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

- If there is no ”adequacy decision” you need to use extra safeguards to make the transfer/disclosure legal

- Usually used safeguard: Commissions Standard Contractual Clauses attached to the agreement
  - EU Case Law: you may still need to implement extra safeguards depending on the country’s legislation and practise conserning data protection (f.ex pseudonymisation, encryption)


DATA SUBJECT RIGHTS

DATA SUBJECT RIGHTS

Right to be informed

- right to be informed of the collection and processing of their personal data. Be transparent!
- You can use university's template, that includes all the necessary questions: link to Flamma
- feel free to use imagination how to present the information

Access Right

- Right to know whether the controller processes personal data concerning the data subject
- The data subject have the right to have access and/or a copy of his/her personal data

Right to Erasure

- In certain cases, the data subject has the right to have the data erased, e.g. if:
  - the processing is based on consent and the consent is withdrawn
  - you no longer need the data for the purposes it was collected
  - the data subject have objected to the processing, and it can be concluded that the processing is not necessary for your research

Right to object

- If the processing is based on public interest, the data subject have the right to object to the processing
- You then need to assess, whether the processing of the data in question is necessary and decide that:
  1. The processing can/need to stop OR
  2. demonstrate that the processing is still necessary (there are compelling legitimate grounds to process the data that override the interests of the data subject)

WHERE TO FIND MORE INFORMATION?

IMPORTANT LINKS (TO FLAMMA)

UH Data Protection Principles

General guidance for processing of personal data

Contract templates can be found on this page (right side of the page)

Researchers' guidance for processing of personal data

Tools and templates can be found on this page (right side of the page)