Data protection in a nutshell
9.10.2020

Data protection officer Jukka Tuomela
Legal counsel Olli Repo
Data protection specialist Anna Rytivaara
Presentation themes

• GDPR
• Basic concepts
  • Personal data & indirect identifiers
  • Special categories of personal data
  • Pseudonymous and anonymous data
  • Processing activities
  • Roles
• The principles of data processing
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.

• The rights of the data subjects

• Processing easy within EU/EEC due to common legislation

• **Data transfer outside EU/EEC restricted**
  • Depends on the level of data protection in the receiving country
What counts as personal data?

- Concept of personal data is very extensive
- Personal data refers to any information by which an individual (the “data subject”) is identified or may be identified **directly or indirectly**
  - in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, an opinion, a job title, image or audio, or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.
- NB! Combining pieces of information may also lead to identification

→ Any piece of information can be personal data
Indirect identifiers

• In addition to name and address, personal data can be, among other things
  • Photo of a car’s registration plate
  • Story of one’s career path
  • Voice/photo/video
  • Hobby
  • Favourite hockey team
  • Title (DPO, President of the University)
  • Names of one’s siblings
  • Blood/muscle sample
  • Any 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 one can connect to a person (interviews, observations, opinions, videos/photos of landscape or buildings etc.; i.e. also with no people in them)
→ Sufficient that one’s colleague, acquaintance or relative can identify a person with the (piece of) information
Special categories of personal data

- **Special categories of data** are those revealing
  - racial or ethnic origin,
  - political opinions,
  - religious or philosophical beliefs,
  - trade union membership,
  - genetic or biometric data which are processed for the purpose of uniquely identifying a natural person,
  - data concerning health
  - data concerning a natural person's sex life or sexual orientation.

- **Forbidden to process these – scientific research an exception**

- **Require additional measures to secure data protection and data security**

- Also social security number and classified information require additional security
Pseudonymous and anonymous data

Pseudonymised 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
  • Pseudonymised personal data is still personal data and subject to data protection legislation

Anonymised 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; anonymisation, 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 anonymisation, 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 pseudonymised data, not anonymised

Processing activities

• Any operation or a 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 and storage,
  • analysis
  • organisation, structuring, adaptation, alteration, combination
  • use, disclosure, dissemination
  • erasure or destruction

• What kind of personal data will you process in your research?
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 university research, the university is typically the controller (alone or with other research organizations)
  • University employer is doing research, research is publicly funded,

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

• Students are usually controllers in their own research for Master’s degree or PhD thesis.
The principles of data processing

• Lawfulness, fairness, transparency
• Purpose limitation
• Data minimisation
• Accuracy (quality of data)
• Storage limitation (time of processing)
• Integrity and confidentiality (access, data security)
• Accountability in compliance (documentation)
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

• Bases of processing of special categories of data ("sensitive data") are stipulated in Art. 9 of the GDPR.
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 with the principles must be demonstrated → the importance of proper documentation
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 an encrypted hard drive.
• Never reveal personal data to others
• 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: 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”

www.tuni.fi/research-data-protection
Thank you!

Questions?

dpo@tuni.fi