# General Data Protection Regulation (GDPR) – Experiences of universities since entering into effect of regulation – How are universities tackling the practical issues

BESTPRAC WG3 Meeting
Belgrade, Serbia
September 25, 2018

Niina Mikkonen
Legal Counsel, Aalto University (Helsinki, Finland)

# GDPR at Aalto University

# What has been done so far

- **Task Force** for GDPR project management
- Data protection officer (**DPO**) – appointed as of 1.1.2018
- Data protection e-learning tool: **online course** "Basics in data protection" – launched during the spring 2018
- Aalto **Personal Data Policy** – adopted in May 2018
- **Information security policy** – under review
- **Data retention policy** – under review
- **Data breach notification system** – Co-operation between DPO and IT security team agreed
- **Data subjects access rights process** – under preparation
- Finnish universities joint **Code of Conduct for learning and research** – under preparation
- **Privacy notices** for different purposes (e.g. employee, student, research, event management, aalto.fi -website)
- **Practical data protection guides** issued to different target groups (e.g. teachers, researchers, HR)
- **PIA** (privacy impact assessment) **policy and guidelines** – in preparation phase
- **DPA** (data processing agreement) – special project to get the DPAs done ongoing (more than 100 agreements needed)
- **International data transfers** (outside EEA) – processes under preparation
- **Security** – processes and routines in field of IT security created and Aalto-website has been run by an external partner for quality assurance and the security of the site and the handling of data has been security tested by external security partner
- Several **workshops and training sessions** have been organized for different target groups of Aalto

# GDPR and research at Aalto University

# Taking personal data and data privacy into account in research

# Aalto's guidance to researchers

# Ascertain that you are processing personal data

- Personal data is all information relating to **an identified or identifiable natural person**, e.g. a name, an identification number, location data, an online identifier or a factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- More information, see: “What is personal data?” https://tietosuoja.fi/en/what-is-personal-data

# If you process personal data in your research, take the following steps and pay attention to following points

# 1) Define the legal basis for processing of personal data

- As mandated by GDPR, the processing of personal data must always be done under one of **the legal bases for processing**
- In scientific research, the basis is usually
  - The processing is "**necessary for the performance of a task carried out in the public interest**"
  - The processing is based on "**consent**"
- The chosen legal basis has an effect on, e.g. to rights of the study participant
- If the legal basis for processing is consent, the participant must have the right to **revoke** it
- **Because the completion of the research should not be endangered, it is advisable to use "the performance of a task carried out in the public interest" as the legal basis for processing whenever possible**

# 2) Plan the entire life cycle of data processing

- Including collection, storing, usage, research cooperation, further research, archiving, deletion **before you begin collecting or otherwise processing the data**

- Remember that the **minimization of data** is part of the general principles of data processing, which means that **only data necessary for the completion of the study** may be collected or otherwise processed

# 3) Ensure that your research participants have been properly informed

- Must be done **before you start collecting personal data** (other processing of personal data)
- Ensure that the data processing has been **described uniformly** in the ”research and research data management plan” and in the ”privacy notice”
- Use **Aalto’s privacy notice documents**:
  - If you collect data directly from research participants: “**Participation confirmation**” and “**Personal data directly from data subjects**”
  - If you receive personal data from somewhere else (e.g. Aalto’s cooperation partner or register): “**Personal data from third parties**”
- Send your privacy notices to tietosuojailmoitukset@aalto.fi

# 4) Document the systems used for storing and otherwise processing of personal data

- An **internal record** to track how data is processed
- Use Aalto's template "**Record of processing activity**"
- Send it to tietosuojailmoitukset@aalto.fi together with privacy notices

# 5) Ensure data security and use only Aalto-approved information systems

- Please see **Aalto IT service's guidelines** on the subject (guide to data protection and information security)

- **A list of all information systems approved by Aalto** for use in processing personal data can be found on Aalto IT service's quick guide "classicification and services related to data"

# 6) Research that deals with sensitive personal data

- **Sensitive personal** data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

- **Aalto Research Ethics Committee's ethical pre-evaluation** must be done before beginning processing activities related to sensitive personal data

# 7) Data protection impact assessment (DPIA)

- Must be must be completed if the planned data processing poses a **substantial risk to the data subjects** (the study participants)

- This may be the case in situations such as when **large amounts of data** is being processed or when the data being processed **pertains to children or is otherwise sensitive in nature**

- This obligation **may be deviated upon on the part of research in the new Finnish data protection legislation**
  - This will be confirmed once the law is complete

# 8) Data processing done outside of Aalto

- If **personal data is sent outside of Aalto to be processed**, a Data Processing Agreement (or other agreement) must be signed with the other party
- Use **Aalto's templates**:
  - If external party is processing personal data **on behalf of Aalto** for purposes defined by Aalto (e.g. subcontractors or could services): "**Data processing appendix** (**DPA**)"
  - If personal data is transferred to other university or research organization and these two parties define the purposes of processing personal data **together**: "**Joint controller agreement**"
- If personal data is transferred to other university or research organization in a way that the other party defines the purposes of processing personal data **by itself**, make sure that e.g. **purpose of use and informing of research participants is agreed before transferring of personal data**
- Personal data can be **transferred outside of the EEA only when certain conditions are met**. More information: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en
- Send signed agreements to tietosuojailmoitukset@aalto.fi

# 9) If you encounter a need to change the way you are processing personal data

- Personal data may be processed **only in the ways that the research participant has been informed** that it will be processed before the processing commences

- If you encounter a need to change the way you are processing personal data throughout the duration of your study, **all required documentation must be recompleted and the data subjects informed of the change**

# 10) In addition

- Familiarize yourself with **the best practices of processing personal data in your own field of research**

- Familiarize yourself with **Aalto's privacy policy**

- If you need further assistance, please **contact your school's legal counsel or Aalto's data protection officer** (dpo@aalto.fi)

# Comments or questions?

# Thank you ☺

**Niina Mikkonen**

**Legal Counsel**

**Aalto University (Finland, Helsinki)**

**Phone: +358 50 366 7352**

**Email: niina.mikkonen@aalto.fi**

http://www.aalto.fi/en/