The new General Data Protection Regulation (GDPR) – Relevance and points of attention for universities

General introduction, impact on universities and actions at Aalto University

BESTPRAC WG3 Meeting
Bucharest, Romania
February 9, 2018

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

Why data protection?

- Safeguarding the fundamental right to privacy
- Setting the frame for legal use of personal data by organizations, companies, public authorities, etc.
- Promoting risk-based and proactive planning of personal data processing and sanctioning breaches of data protection regulations

What is GDPR?

General Data Protection Regulation (GDPR, 2016/679) adopted by the EU Parliament

- Into force 25 May 2018
- Applied as such in all EU countries

https://gdpr-info.eu/

National regulation by Data Protection Act

- By May 2018

GDPR is evolution not revolution

Applies to organizations carrying out activities within the EU	**Risk based approach and accountability**	**Data subjects have more control over their own personal data**
Data Protection Officer	**Data breach reporting**	**Sanctions for breaches**

GDPR terminology: Personal data, Data subject

Personal data – Data subject

- **Personal data** = Any information **relating to an identified or identifiable natural person** (“**data subject**”)
- An identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**
- Single peace of information or a set of information
- E.g. voice, a video, an e-mail address, a car registration number, a social security number, a passport number, computer IP address, credit card number, fingerprints, photo, health records or **a combination of significant criteria which allows him to be recognized by narrowing down the group to which he belongs** (age, occupation, place of residence, etc.)

GDPR terminology: Processing

- Obtaining, recording or holding information or data on individuals
- Carrying out **any operation or set of operations** on this information or data, including (but not limited to)
  - Collection, storage, organization, amendment
  - Disclosure of the information or data by transmission, dissemination or otherwise making available, or
  - Blocking, erasure or destruction of information or data

GDPR terminology: Controller, Joint controllers

Controller

- 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**
- E.g. university research group interviews data subjects in the research project for the scientific purposes stated in the research plan

Joint controllers

- Two or more controllers **jointly determine the purposes and means of processing**
- An agreement must be concluded between the joint controllers: “They shall in a transparent manner determine their respective responsibilities for compliance with the obligations”
- Joint responsibility to be excluded
- E.g. research consortium collects and shares personal data in the research project

GDPR terminology: Processor

- A natural or legal person, public authority, agency or other body which **processes personal data on behalf of the controller**
- E.g. university receives personal data from and on behalf of other research organization in the research project
- Employee of the controller is not a processor – employee's work is part of controllers activities

Controller

- **Responsibility to inform data subjects**
- **Accountability**
- **Notification of personal data breaches**
- **Responsibility of the data security**

Processor

- **Processing in accordance with the instructions of the controller**
- **Notification to controller of personal data breaches**
- **Responsibility of the data security**

Outsourcing the processing of personal data: Data Protection Agreement

When processing is to be carried out on behalf of the Controller by external contracted third party (Processor), **an agreement must be concluded** which sets out

- Subject-matter and duration of the processing
- Nature and purpose of the processing
- Type of personal data and categories of data subjects
- Obligations and rights of the controller

Sufficient guarantees to implement appropriate technical and organizational measures to meet the DGPR requirements – **Data Protection Agreement (DPA)** (or equivalent)

Legal basis for processing of personal data

Processing shall be lawful only if at least one of the following applies:

- **Consent** given by the data subject: freely given, specific, informed and unambiguous indication of his/her wishes
- Necessary for **the performance of a contract** to which the data subject is a party
- Necessary for **compliance with a legal obligation** of the controller
- Necessary in order to **protect the vital interests of the data subject**
- Necessary for **public interest/official authority**
- Necessary for **legitimate interests**, except where overridden by rights of the data subject

Principles relating to data protection

Lawfulness, fairness and transparency

Processed **lawfully, fairly and in a transparent manner** in relation to the data subject

Purpose limitation

Collected for **specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes

Data minimisation

Be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed

Accuracy

Be **accurate** and, where necessary, **kept up to date**; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are **erased or rectified** without delay

Principles relating to data protection

Storage limitation

Be kept in a form which permits identification of data subjects for **no longer than is necessary** for the purposes for which the personal data are processed

Integrity and confidentiality

Processed in a manner that ensures **appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Accountability

Responsible for, and be and be able to demonstrate **compliance with the GDPR**

Data protection by design and by default

At the time of the determination of the means for processing and at the time of the processing itself implement **appropriate technical and organisational measures**, which are **designed to implement data-protection principles**

Rights of the data subjects

- Information on collection of personal data
- Access to the data
- Rectification of inaccurate personal data without undue delay
- Erasure (right to be forgotten)
  - Exceptions: Research, Archiving, Public interest
- Data portability - right to transmit data to another controller
- To deny to be subjected to automated decision processing, including profiling

Information to data subjects (Privacy notice)

Information provided when personal data collected from data subjects:

- Identity and the contact details of the controller
- Contact details of the data protection officer of the controller
- Legal basis for processing personal data and purpose of use
- Recipients of the personal data, if any
- Whether personal data is intended to be transferred outside EU/EEA area
- Period of storage of the data or the criteria for determining it
- Existence of the rights of the data subject
- Existence of automated decision-making, including profiling, if relevant

Additional requirements if personal data is collected from other sources

International personal data transfers

- Only transfer personal data to countries deemed "adequate" by the EU
  - http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

- Safeguards must be agreed and in place prior to transfer
- Binding corporate rules may be used within an international organization
- EU-US transfers subject to separate agreement

Breach reporting and penalties

Breach notifications

- Mandatory notification to the supervisory authority
- When the breach is likely to "result in a risk for the rights and freedoms of individuals"
- **Within 72 hours** of first having become aware of the breach
- In case of a high risk, to the data subject
- Data processors also required to notify breaches to controllers "without undue delay"

Fines for GDPR breaches are possible

- Effective, proportionate and dissuasive
- Imposed by the supervisory authority
- **Max. 20 M€ / 4 % of turnover**

Action points: Identify your registers and document

Which work functions involve dealing with personal data?

Which data systems, registers and files data is restored in?

Why are you holding the data?

Who is responsible of the data system, register or file?

Why was it originally gathered?

Is all data relevant and necessary for the specific functions?

How did you obtain it?

How long will you retain it?

How secure is it, both in terms of encryption and accessibility?

Do you ever share it with third parties and on what basis?

Do you inform about the processing of personal data?

Check your registers' GDPR compliance

- Check that each of the registers have **lawful basis** for processing personal data
  - If not, erase the data/register
- Check that the register is **appropriately secured**
  - Consider both technical (IT-security) and organizational aspects (access rights)
- Check that person responsible for the register has **sufficient understanding** about GDPR requirements
  - If not, training/guidance needed

Check your registers' GDPR compliance

- Check that for each register
  - **Records of processing activities** (internal documentation) has been created and is up to date
  - **Privacy notice** (information to data subjects) has been created, is up to date and available for the data subjects
- Plan how to handle **requests by data subject(s)**
- Ensure that you and personnel of your organization is **familiar with procedures** in place to report and investigate personal data breached

Check your registers' GDPR compliance

- Check if any **data processor(s)** are engaged
  - If yes, make sure that written Data Processing Agreement is in place with the processor at latest in May 2018
- Check if there are any **international data transfers** related to your register
  - If yes, and in case the transfers are outside the EU/EEA make the necessary actions
- Ensure that you processes include GDPR compliance steps and principles for **designing personal data processing** are in use

GDPR implementation at Aalto University

Organization and responsibilities

- Task Force for GDPR project management
- Data protection officer (DPO) appointed on 1.1.2018

GDPR Policies, Guidelines and Templates

- Aalto GDPR Policy
- Code of Practice for Research Data Protection at Finnish Higher Education Institutions (HEIs)
- Code of Practice for Study Data Protection at HEIs (update)
- Aalto IT Policies and Guidelines (update)
- Aalto Research Ethics Review guidelines (update and on-line request platform)
- Privacy Notice and Records of Data Processing (update of current and templates)
- Data Balance Sheet
- DPA template
- Participation form for scientific research

GDPR implementation at Aalto University

Review of Aalto personal data management

- Identifying IT-systems/data entities, including data flows and lifecycle
- Defining system/application/data entity owners
- Assessing the need for (and updates on) DPAs and DPIAs

Online platforms created

- Consent document processing platform for researchers
- Access/correction/portability/erasure/complaints request processing platform

Data protection impact assessments (DPIAs)

- On some higher risk systems and applications

Training

- On-line courses, including tests (for staff and students)
- Lectures for units/personnel groups
- Specified training for service staff

Group discussion:

- Actions that universities are taking or planning to have relating to GDPR

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/