The protection of personal data

Legal provisions and practical application

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

What is the GDPR ?

- GDPR (*General Data Protection Regulation)*
  - European Regulation (2016/679) directly applicable in Belgian law and in force as of May 25, 2018

- Additional details on Scientific research are left to the member-states:

- Belgian Law of 30 July 2018 on the protection of individuals with regard to personal data processing

Who’s concerned ?

- 1. Every institution or individual who is established in the EU, who processes personal data (from the EU or not).
- 2. Every institution or individual who is established outside the UE, who processes personal data of European persons for offering goods and services.
- It does include the University and it’s researchers.

A. What is personal data?

- Any information (broadly defined) that can be used to identify, directly or indirectly, one natural person:
  - A name, a number, an online id,
  - Location data,
  - physical, physiological, genetic, mental, economic, cultural or social data.

- Examples:
  - registration for an academic course
  - medical file
  - database of participants
  - business contact
  - picture

A. What is a processing of data?

- In practice, any operation in which personal data is involved, whether it is in electronic or paper format.
  - Collecting
  - Encoding
  - storing
  - Altering
  - Consulting
  - Using
  - Disclosing
  - Destructing ...

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

1st principle: Accountability

- The University takes a legal responsibility for Personal data processing
- It has to take actions to make sure the principles of the GDPR are taken into account
- Data processings have to be described in a register

2nd principle: Privacy by design

- Protecting the rights of the natural persons since the design of the experiment, and until the end of the use of these data (with any technical or organisational measures)
- This means securing digital data (cf. local computing unit - UDI) as well as the data on paper!

3rd principle: Privacy by default

- Use the data only to the extent necessary for the purpose the experiment.
  - Only needful data is collected
  - It is not kept longer than necessary
  - It is only used for the research that has been announced
  - It is available only to the researchers involved in the experiment
  - Security measures are taken and put into action.

Principle of minimization

4th principle: lawfulness of processing

- Justify the lawfulness of each processing:
  - ***Consent (free and informed)***
  - *Legal obligation*
  - *Execution of a contract*
  - *Protect the vital interests of a person*
  - ***Public mission** / exercise of official authority*
  - *legitimate interests of the Controller*
- (Soon-to-be) Available templates will make this choice easier

5th principle: Data subjects have rights

- Access to Processing information and data
- Rectification of data
- Erasure (right to be forgotten)

Specific rights:

- *Restriction of processing*
- *Portability of data*
- *Opposition to processing*
- *Do not be subject to an automated decision*

6th principle: Penalties and fines

- Recommendation of the Data protection Authority
- Fines (up to 20M €)
- Legal actions
- Termination of the research.

- In case of problems or doubts, contact the DPO immediately (dpo@uliege.be)

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

Think about GDPR

- How shall I ensure the security of my data?
- How will I get these data?
- Who will have access to it?
- What shall I do with that data?
- For how long shall I keep it?
- What will be the fate of these data after the experiment?
- Will my research comply with GDPR's principles?

To inform

- Inform the data subjects of the processing of their Personal Data:
  - This include: purposes, legal basis, data used, duration of processing, anonymization, international transfers of non-anonymous data, etc.
  - Standard documents are available on Uliège GDPRs' intranet (or specific document in your Department's intranet)

To conduct Data Protection Impact Assessments

- A written report which evaluates the risk to privacy and how to reduce it
- Only when *fundamental rights and freedoms* of the data subject could be at risk (to be determined with the DPO)
- To be carried out by the researcher

Subcontractors and collaborations

- If you use subcontractors or if you transfer non-anonymous data outside the University, you must ensure compliance with the legal rules on data protection.
- Collaborations with partners outside the UE should raise maximum concern
- Contact the Legal Department for assistance.

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

Data breach, corruption or loss

- These are personal data violation cases, which could lead to penalties and fines
- To do:
  - Secure data
  - Notify the DPO of the incident (dpo@uliege.be)
  - Report the incident to the Data Protection Authority (with the help of the DPO)
  - Notify the persons concerned
- In case of problems or doubts, contact the DPO immediately (dpo@uliege.be)

Requests to exercise rights

- Make sure it comes from the data subject
- Follow-up within 30 days
- There are exceptions for research (but legal analysis has to be done on a case-by-case basis)
- Animals and dead people don’t have these rights
- In case of specific requests, do not hesitate to ask for an advice (dpo@uliege.be).

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

Erase or make anonymous

- Personal data must be erased when the experiment is over.
- Exceptions are possible under strict conditions
- Anonymizing data (full anonymity) is a way to keep data longer

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

How to secure data ?

- Ensure that computer data is secure:
  - Passwords, passwords, passwords !
  - Data on an encrypted hard disk or on disk space managed by SeGI (request via your UDI), e.g. DOX
  - No personal data on USB sticks (which tend to get easily lost...)
  - No personal data by email, including attached files!

How to secure data ?

- 3 levels of anonymity:
  - Fully nominative
  - Fully anonymous
  - The in-between: pseudonymized
- To assign a code to each participant and to keep it in a secure database
- Less severe troubles in case of a data breach
- Deleting the secure database is a convenient way of anonymizing data

How to transfer data between colleagues ?

- Only through secure and dedicated channels, e.g. a medical file or sensitive information should NOT be sent as a simple attachment by email
  Use DOX sharing or other SeGI managed disk space
- Only when necessary, and to the extent necessary (put expiry date for sharing with DOX)
- *You may be held liable.*

How to secure data on paper ?

- Keep only what is necessary for the stated purpose, or what must be kept legally. The rest must be destroyed.
- Throwing it in the garbage doesn't mean destroying.
- Keep in secure areas (locked cabinet, office with restricted access).
- Sort on a regular basis.

Open repositories ?

- No non-anonymous data (exceptions under strict conditions)
- It is not sure that pseudonymized data can be publicly accessible
- Anonymous data is ok:
  - Change the code of the pseudonymized data
  - Make sure that data doesn’t allow for a re-identification.
  - In case of doubts, contact the DPO (dpo@uliege.be)

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

Practical cases

- For my study, I have to set up a group of volunteers for tests. What do I need to think about to be in order with regard to the GDPR?

Practical cases

- For my study, I have to set up a group of volunteers for tests. What do I need to think about to be in order with regard to the GDPR?
  - Legal basis: consent by means of a clear form
  - Storage period: until the final report is completed (or data anonymised)
  - Only the necessary data
  - No transmission of data to third parties
  - Securing the collected database (via duplication of databases and coding) + use of an encryption solution
  - Clear procedure for unregistering

Practical cases

- One of the participants in my study asked to withdraw from the research project. What to do with his or her personal data?

Practical cases

- One of the participants in my study asked to withdraw from the research project. What to do with his or her personal data?
  - Two simple possibilities:
    - 1. delete them
    - 2. make them anonymous
  - In some cases, it is possible to refuse to exercise a right, but this implies a prior legal analysis, hence the importance of thinking about this point when designing the project.

Practical cases

- The personal data collected as part of my study on the spread of the ebola virus is of interest to my colleague who works on the influenza virus. Can I send them to him?

Practical cases

- The personal data collected as part of my study on the spread of the ebola virus is of interest to my colleague who works on the influenza virus. Can I send them to him?
  - A priori, scientific research is always a compatible finality. However, it might be interesting to consider, from the very beginning, a sufficiently broad finality covering several potential research projects (and therefore a single consent). In this case, re-employment may be acceptable as long as the persons concerned are informed.

The protection of Personal Data

- A. Introduction
- B. Principles
- C. In practice – before the experiment
- D. In practice – during the experiment
- E. In practice – after the experiment
- F. Specific questions
- G. Practical cases
- H. Q&A

Pierre-François Pirlet (dpo@uliege.be)

Privacy intranet : https://my.rgpd.uliege.be


LIÈGE
université