LIÈGE université

Working with personal data ? Think GDPR!

Legal and practical aspects

Working with personal data ? Think GDPR!

- Introduction
- 6 Principles
- Points of attention
- Specific questions
- Q&A

What is the GDPR ?

- GDPR stands for *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.

What is personal data?

- Any information that can be linked to a natural person
  - Directly (name, patient number, online id) or
  - Indirectly (by combining several data).
  - Personal data can be every data that could be used to identify someone: physical, physiological, genetic, mental, economic, cultural or social data.

- Personal data are everywhere:
  - registration for an academic course
  - medical file
  - database of participants
  - GPS data
  - Human tissues (w/ an identifier tied to a natural person)

Processing of data? What does this mean ?

- Any operation in which personal data is involved is a processing, whether it is in electronic or paper format.
  - Collecting
  - Encoding
  - storing
  - Altering
  - Consulting
  - Using
  - Disclosing
  - Destructing ...
- All these operations fall into the scope of the GDPR.

Working with personal data ? Think GDPR!

- Introduction
- 6 Principles
- Points of attention
- Specific questions
- Q&A

1st principle: Accountability

- The University takes a legal responsibility for your processings of Personal data. This means that, in case of problems, the University will be accountable for your processings.
- But you have to follow some rules to make sure your processings are GDPR-compliants.

2nd principle: Privacy by design

- You have to protect the privacy of the data subjects since the design of the experiment, and until the end of the use of these data. This means using every technical and organisational technique available.
- This means securing digital data as well as the data on paper!

3rd principle: Privacy by default

- Do I really need that personal data ?
- Make use of the minimization principle:
  - Only collect needful data;
  - Do not kept it longer than necessary;
  - Use it only for the research that has been announced;
  - Share it only with the researchers involved in the experiment;
  - Enforce security measures.

4th principle: lawfulness of processing

- There are six “scenarios” which allows the lawful use of personal data:
  - *Legal obligation*: it’s written in a law;
  - *Execution of a contract*: I need the data for the contract (concluded with the data subject);
  - *Protect the vital interests of a person*: medical emergency;
  - *legitimate interest of the processor* (not to be used in research !)
  - ***Public mission*** : fundamental research is a public mission – To be chosen when an “ethical consent” is also sought
  - ***“GDPR” Consent (free and informed)***
- Templates are available to make this choice easier

5th principle: Data subjects have rights

- Access: “What data about me are you using ?”
- Rectification of data: “Please correct my data in your files”
- Erasure (right to be forgotten): “Please delete my personal data in your files”

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 against the University and/or the researcher
- Termination of the research.

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

Working with personal data ? Think GDPR!

- Introduction
- 6 Principles
- Points of attention
- Specific questions
- Q&A

Think about GDPR from the beginning

- 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 the principles of the GDPR?

Think about GDPR from the beginning

- Using https://www.dmponline.be/
- A free tool designed to easily draw up *Data Management plans*, as required by some funding agencies
- GDPR template available: specific questions to help you design a documentation of your processing of personal data
- Might become mandatory to draw such a DMP for every research project (specific training available through the R&D administration of ULiège – next session: Nov. 26th)

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 templates are available on the intranet of the University (https://my.rgpd.uliege.be) - or specific templates in the intranet of your Department.

To conduct Data Protection Impact Assessments

- A what ? A written report which evaluates the risk to privacy and how to reduce it
- When ? 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 (check the intranet and dmponline.be)

Subcontractors and collaborations

- If you make use of 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.

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).

After the study: 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

Working with personal data ? Think GDPR!

- Introduction
- 6 Principles
- Points of attention
- Specific questions
- Q&A

How to secure data ?

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

How to secure data ?

- Assign a code to each participant and keep it in a secure database
  - Less troubles in case of a data leak
  - Deleting the secure database is an easy way of anonymizing data
  - Caution: pseudonymous ("coded") data is not anonymous data. GDPR still applies.

Do not forget personal data on paper !

- Keep only what is necessary for the study, or what must be kept legally. The rest must be destroyed.
- Throwing it in the bin doesn't isn’t enough: destroy the data!
- Keep in secure areas (locked cabinet, office with restricted access).
- Sort on a regular basis.

Open repositories ?

- Do not give access to non-anonymous data (exceptions under strict conditions)
- 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)

Working with personal data ? Think GDPR!

- Introduction
- 6 Principles
- Points of attention
- Specific questions
- Q&A

LIÈGE
université

Pierre-François Pirlet (dpo@uliege.be)

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

LIÈGE université