Working with personal data ? Think GDPR!

Legal and practical aspects

Outline of the presentation

- GDPR in a nutshell
- What to do when…
- Questions and (hopefully) answers

GDPR in a nutshell

- Personal data?
- Any information (in the broadest sense) that makes it possible to identify, directly or indirectly, a natural person:
  - a name, an online identifier, a code number;
  - a set of data sufficiently precise to re-identify a person (e.g. rare health condition)
- Anonymous data ≠ Personal data

GDPR in a nutshell

- Special (sensitive) categories of data:
  - information relating to ethnic origin,
  - sex life or sexual orientation,
  - religious/philosophical beliefs,
  - political opinions,
  - trade union membership,
  - **physical/mental health,**
  - **genetic data,**
  - biometric data when used to identify a person,
  - criminal offences and convictions
- Require another layer of security

GDPR in a nutshell

- The GDPR provides a framework for the *processing* of personal data
- Processing: any operation involving personal data, whether in electronic or paper form:
  - collection
  - encoding
  - storage
  - change
  - consultation
  - use
  - disclosure on a more or less large scale
  - destruction ...

GDPR in a nutshell

Risk analysis and security

- Think about the use and security of the data *before* collecting it.
- Data processing operations must be described in a register.
- If significant privacy risk, conduct a *Data Protection Impact Assessment.*

Https://dmponline.be/

(Uliège GDPR template available)

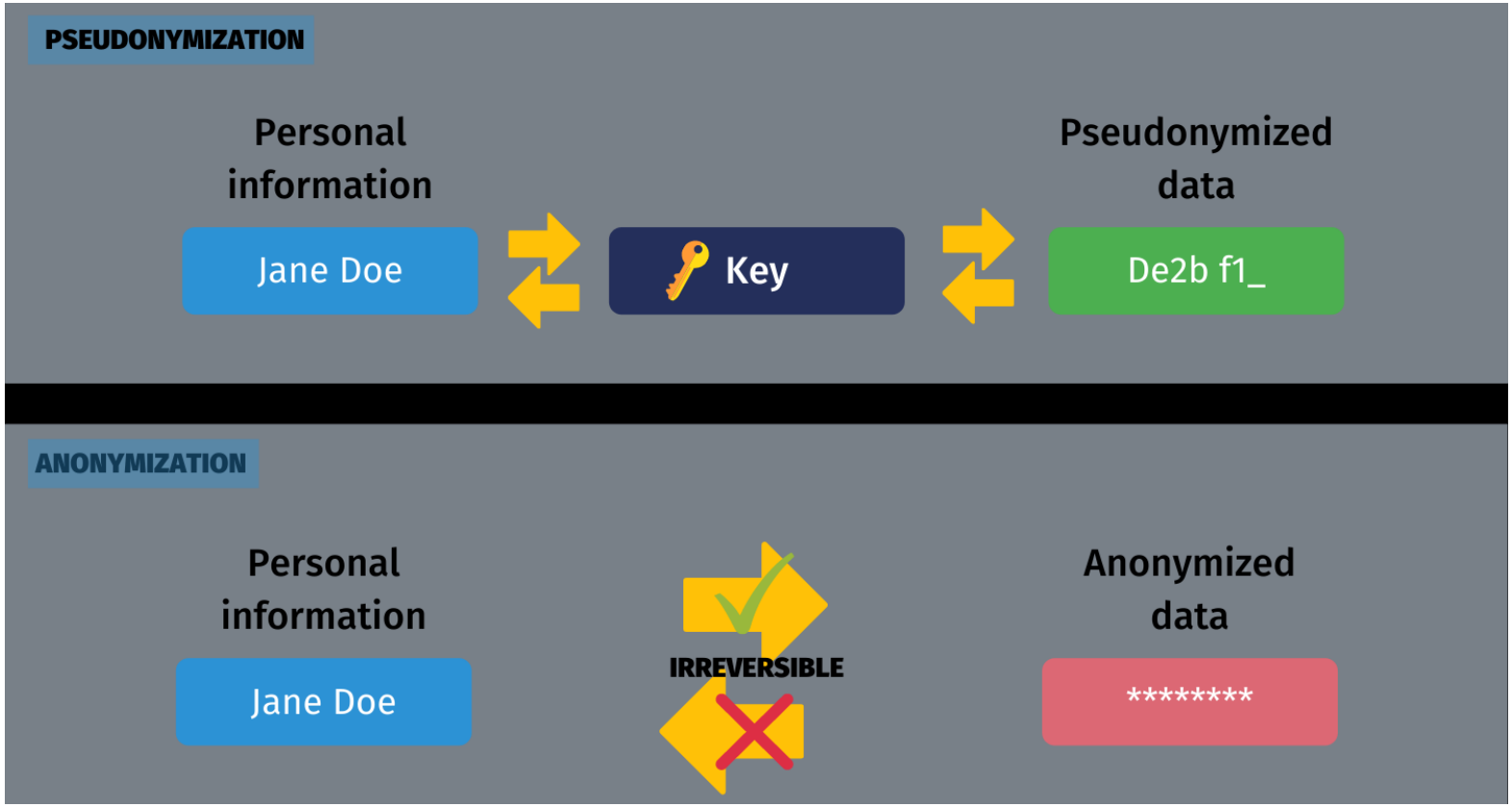
GDPR in a nutshell

Principle of minimization & privacy by default

- Use the data only to the extent necessary to achieve the purposes of the processing:
  - Only the necessary data is collected
  - It shall not be kept longer than necessary
  - It shall be used only for the purpose that was announced.
  - It shall only be accessible to the researchers participating in the experiment.

GDPR in a nutshell

When possible, use pseudonymization or anonymization



GDPR in a nutshell

Lawfulness of processing

GDPR in a nutshell

Inform

- Make sure that you systematically inform the data subjects of the use that will be made of their data:
  - Types of data, purposes, duration and nature of processing
  - Their rights about their data
- Templates are available:

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

GDPR: what to do when… ?

What should I do when… ?

GDPR: what to do when… ?

… I plan a direct collect of personal data ?

- Direct collect = collecting data by interviewing or observing subjects.
- 4 obligations:
  - Beforehand, assess risks induced by processings those data
  - Determine the legal ground
  - Inform
  - Entry into the record of processing activities (more to come in the coming months about this)

GDPR: what to do when… ?

… I plan an indirect gathering of personal data ?

- Indirect gathering = Reuse of data from other studies, from another controller, from a "public" source (website)
- 4 obligations already stated (analyze & securize, legal ground, inform, record)
- Check if, from a legal standpoint, the re-use of these data is allowed

GDPR: what to do when… ?

… I plan to process special categories of personal data ?

- Some data is more sensitive:
  - racial or ethnic origin;
  - political opinions, religious or philosophical beliefs or union membership;
  - genetic data;
  - Biometric data for unique identification purposes (e.g. fingerprint data or facial or iris recognition);
  - health-related data;
  - sexual life or sexual orientation; criminal convictions and offenses;
- 4 obligations already stated (analyze & securize, legal ground, inform, record)
- Compliance with the exemptions in Article 9 of GDPR
- *Data Protection Impact Assessment* if there is a risk over the privacy.

GDPR: what to do when… ?

… I plan to send datasets containing personal data to public repositories ?

- The public availability of data must be considered
- Only strictly anonymous data (not pseudonymized!)
- Identifying or pseudonymized data only if formal agreement of the data subjects (must remain an exception).

GDPR: what to do when… ?

… I plan to collaborate and share data with another organization?

- Sharing and processing personal data between several research institutions means specific obligations
- 4 obligations already stated (analyze & securize, legal ground, inform, record)
- Legal analysis of the status of each partner and the rights and obligations of each.
- Legal agreement always required.

GDPR: what to do when… ?

… a subcontractor will process data on my behalf?

- It is also a specific case (e.g. a lab from the UCLouvain will conduct a statistical analysis of my data)
- 4 obligations already stated (analyze & securize, legal ground, inform, record)
- Legal analysis of the mission of the subcontractor and the rights and obligations of each party.
- A legal agreement is also required.

GDPR: what to do when… ?

… I plan to send personal data abroad?

- E.g. collaboration with a research center in Switzerland; storage of data in the United Kingdom.
- 4 obligations already stated (analyze & securize, legal ground, inform, record)
- In the European Union: no particular difficulty;
- Outside the EU: depends on the status of the country concerned
- USA: a priori, currently very complicated
- Contact your legal department
- Beware of *cloud* storage: where are the datacenters?

GDPR: what to do when… ?

… I receive a request for deletion or withdrawal of consent?

- A data subject requests to have his/her data deleted from your databases.
- Legal analysis required but in most cases, proceed with deletion.
- 30 days delay (extendable by 30 days)
- Anticipate to avoid complaints.

GDPR: what to do when… ?

… there is a *data breach?*

- Data accidentally made public or modified, or erased.
- Risk of sanctions and fines: act fast.
- To do:
  - Secure personal data as much as possible
  - Have your DPO informed
  - Report the incident to the data protection authority (with the help of the DPO)
  - Notify the data subjects
- If you have any problems or doubts, contact your DPO immediately (dpo@uliege.be) .

GDPR: what to do when… ?

… my research is over?

- When the goals (*purposes)* of the data processing are achieved, in principle, deletion.
- Delete or make anonymous?
- No keeping without a defined purpose that has been announced to the data subjects: anticipate !

GDPR: what to do when… ?

… I want to recruit a participant via an online form?

- Avoid using Google Form, as it is a (US) third party tool
- Use the “enquêtes" tool or a tool installed on a GIGA server
- Provide an information and consent document
- Provide a click button or check box to validate consent to participate in the study.

Note: an online consent does not have the same force as a paper consent.

GDPR: what to do when… ?

… I want to share raw personal data with my colleagues?

- share only what is necessary to complete the study
- share in a secure way: share a document via Dox and password, or via a specific software
- do not put an excel file on a directory shared with the whole department!

You could be legally responsible for a data leak !

GDPR: what to do when… ?

… I need to handle large files containing personal data?

- This data must be protected against loss of confidentiality
- Use passwords or even encrypt the hard disk
- Do not multiply the copies of datasets (more copies = more risk)

GDPR: what to do when… ?

… there's a lot of personal data on my computer ?

- 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!

GDPR: what to do when… ?

… there's a lot of personal data on my computer ?

- 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.

GDPR: what to do when… ?

… there's a lot of personal data on paper in my office ?

- 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.

Outline of the presentation

- GDPR in a nutshell
- What to do when…
- Questions and (hopefully) answers

Pierre-François Pirlet (dpo@uliege.be)

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


LIÈGE
université