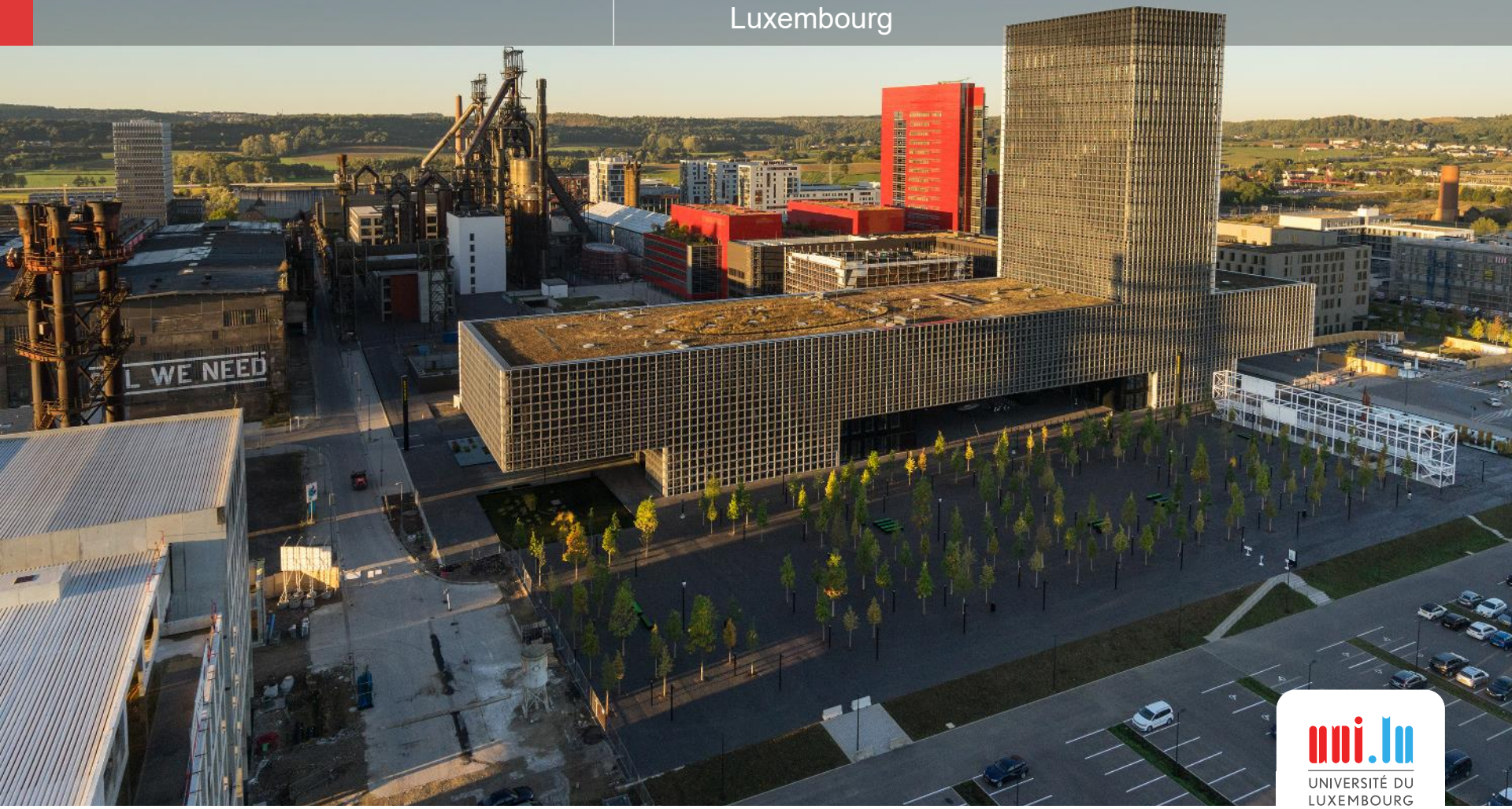
University of Luxembourg

Multilingual. Personalised. Connected.

Towards a guide for researchers in GDPR implementation

Dr Sandrine Munoz, Data Protection Officer at University of Luxembourg



UNIVERSITÉ DU LUXEMBOURG

The risks of GDPR non compliancy: some examples

- July 2018: **400.000€** fine suffered by an hospital in Portugal for GDPR breach
  - Access of hospital's staff and other professionals to patient data through wrong profiles (**Deficient profile management**: 985 registered doctors profiles with only 296 doctors)
  - **Unrestricted access** to all patient files regardless of the doctor's specialty (sensitive data)

⇨ Conclusion of the Supervisory Authority: **no implementation of appropriate technical and organisational measure to protect patient** data

The risks of GDPR non compliancy: some examples

- January 2019: fine of 50 Mio € imposed by the French Data Protection Authority against Google LLC

  https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc

  - Lack of transparency
  - Inadequate information
  - Lack of valid consent regarding the ads personalisation

What does GDPR Implementation for researchers mean ?

- **Different purposes for personal data processing:**
  - Research projects,
  - Communication (e.g. through events, publications),
  - Sharing of personal data with external institutions and users

- **Complex legal framework for research projects**
  - General Data Protection Regulation 2016/679
  - The specific provisions in local laws of controllers in the European Union: the Luxembourg Law of 1st of August about CNPD organisation and implementing the GDPR (specific provisions about research art.62 to 65)

Which changes after May 2018 - Guidance of the European Commission

UNIVERSITÉ DU LUXEMBOURG

Key messages:

- **Clear language in privacy policies**
- **Consent from user:** affirmative consent
- **More transparency:** information of data subjects
- **Stronger rights** of data subjects
- **Stronger enforcement of the Data Protection Regulation**

https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

1. Think GDPR implementation from the start and contact your DPO asap
2. Follow the training sessions offered by the CNPD and your institution
3. Check your institution's data protection policy and guidance
4. Document your compliancy
5. Do not underestimate the data protection contractual aspects
6. Implement appropriate security measures and request advice from CISO

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

7. Inform properly the data subjects of your processing
8. Do not forget data subject rights
9. Share personal data only if legally authorised
10. Check if your project involves performance of a DPIA
11. Check if sharing/transfer of personal data outside the European Union
12. Consider anonymization and pseudonymisation techniques

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

1. Think GDPR implementation from the start and contact your DPO asap

- Check if your institution has a Data Protection Officer and contact him or her for guidance

- Don’t forget that your Chief Information Security Officer is also able to provide advice and guidance about Information Security

2. Follow the training sessions offered by the CNPD and your institution

- Attend regular training sessions of DPO/CISO and CNPD

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

3. Check your institution's data protection policy and guidance

- Read the data protection policy of your institution and comply

4. Document your compliancy

- Each controller or processor shall maintain a record of processing activities under its responsibility
- Your institution can be qualified as controller, processor or joint-controller
- The controller is the one "who" determines the purpose and means for the processing
- E.g your institution decides "why" and "how" to run the processing related to your research project

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

- **In research, some projects** are **carried out by different institutions**, if the purpose and the means are decided jointly the institutions are qualified as **joint-controllers**

- The **processor** is the one who process personal data on behalf of the controller

- **The existence of a processor depends on a decision taken by the controller** to process data within the organisation or to outsource all or part of the processing activities

12 key points that researchers should keep in mind for GDPR compliancy

5. Do not underestimate the data protection contractual aspects

The "magic" standard data protection clause to insert systematically in the contracts does not exist!

- Anticipate data protection in your agreements
- If your institution is controller and your contractor is processor, conclude an agreement as detailed in article 28 of GDPR (ex: service provider for research platform)
- In case of joint-controllership between your institution and another research institution, conclude an agreement setting out the respective responsibilities of each joint-controller in the processing (including the relevant data subjects)

12 key points that researchers should keep in mind for GDPR compliancy

6. Implement appropriate security measures and request advice from CISO

- **Security of processing is mandatory (art.32)**
  - Implement security measures to personal data processing (e.g pseudonymisation, encryption, ongoing confidentiality…)
  - Adapt the security measures to the specificities of your processing (e.g sensitive data, processing at large scale, data of pupils…)

- **Why implementing appropriate security measures?**
  - No appropriate security measures can lead to personal data breach with consequences for your institution and the data subjects
  - Data Protection Authority can impose fines for lack of security measures

UNIVERSITÉ DU LUXEMBOURG

7. Inform properly the data subjects of your processing

- **The data subjects should receive the information in a:**
  - Concise, transparent, intelligible and easily accessible form, using clear and plain language
  - The information shall be provided in writing, or by other means, including, where appropriate, by electronic means

  →This information is provided by a privacy notice or privacy policy
  - Inform participants to research projects
  - If you organise an event do not forget the privacy notice

12 key points that researchers should keep in mind for GDPR compliancy

- Identity and the contact details of the controller
- Purposes of the processing for which the personal data are intended
- Legal basis for the processing
- Period for which the personal data will be stored
- Source of the personal data
- Recipients or categories of recipients of the personal data
- Ways for the data subject to exercise his/her rights
- Right to lodge a complaint with the supervisory authority
- Transfer of personal data to a third country or international organisation
- Contact details of the DPO, if applicable

12 key points that researchers should keep in mind for GDPR compliancy

8. Do not forget data subject rights

- **Existing rights**
  - Right to information about the processing of personal data
  - Right to object to processing activities
  - Right to restriction of processing
  - Right to erasure
- **New rights**
  - Data portability
  - Right to get information in case of a data breach

➡ Do not forget to mention them in privacy notice

➡ Ensure that the data subjects can exercise their rights and provide contact details for that purpose

➡ Contact your DPO for modalities of data subject rights' information and exercise

12 key points that researchers should keep in mind for GDPR compliancy

9. Share personal data only if legally authorised

- Do not share personal data with any third party unless there is a legal ground or/and an appropriate agreement in place

- Sharing with colleagues has also to be justified

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

10. Check if your project involves performance of a DPIA

- If there is potential **high risk to the rights and freedoms of data subjects**, carry out a data protection impact assessment (DPIA) for each processing operation
- DPIAs are tools that help identify and minimize these risks for new projects
- DPIA is mandatory prior to the processing
- One DPIA can be performed for similar processings

12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

An hospital processing its patients' genetic and health data

- Sensitive data
- Data concerning vulnerable data subjects
- Large scale processing → DPIA required

An institution monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc.

- Systematic monitoring
- Vulnerable data subjects

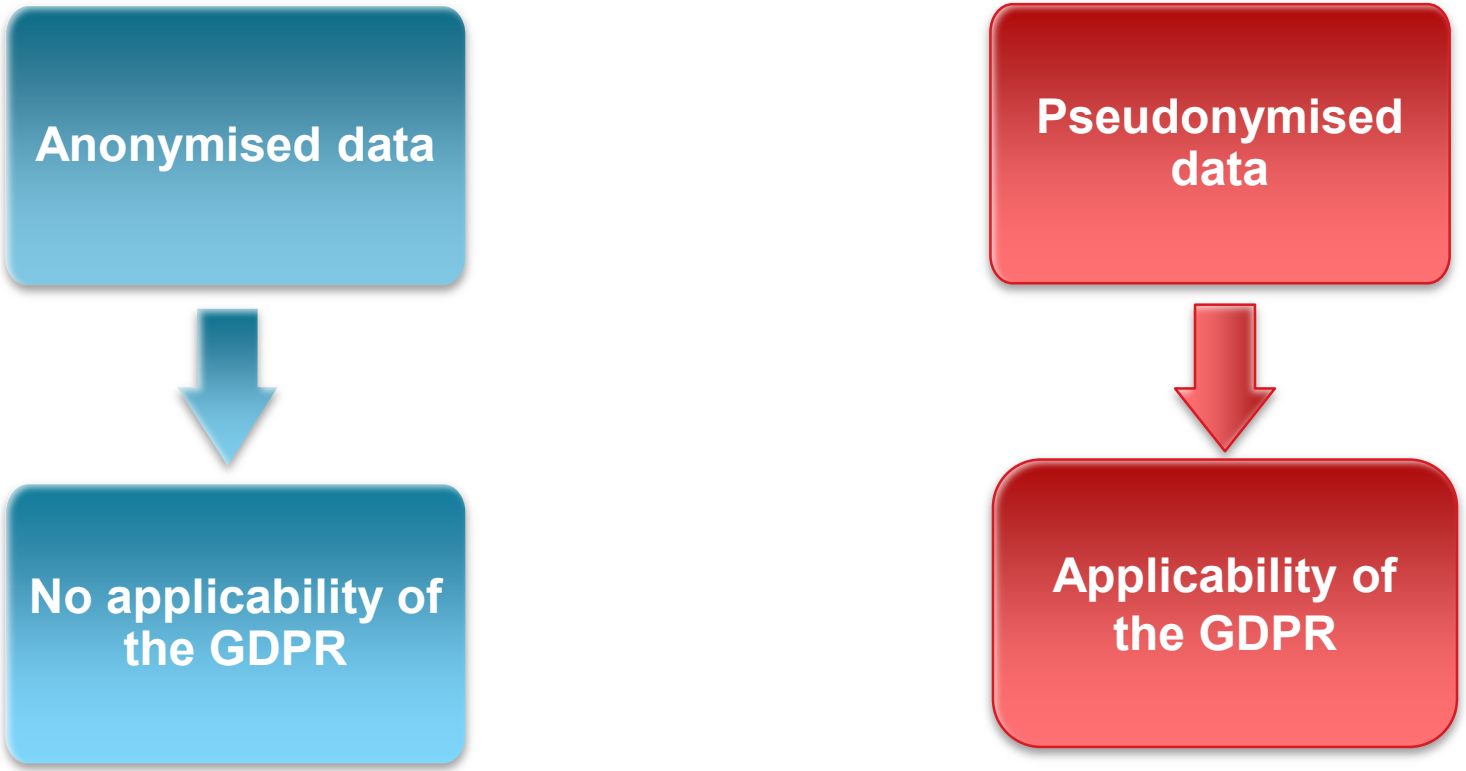
12 key points that researchers should keep in mind for GDPR compliancy

11. Check if sharing/transfer of personal data outside the European Union

- Check if you will share personal data with a partner outside the EU or use the services of a provider located outside the EU
  - Is the partner or the provider located in a country of EEA (Norway, Liechtenstein and Iceland) or offering an adequate level of protection?
  - List of countries offering an adequate level of protection https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en
    - Japon since 23/1/2019
- If not, did the data subject expressly agreed to such transfer (except for massive transfer)?
- Otherwise, you are in a situation of transfer to a third country which requires appropriate safeguards ➡ Consult your DPO

12 key points that researchers should keep in mind for GDPR compliancy

12. Consider anonymization and pseudonymisation techniques



12 key points that researchers should keep in mind for GDPR compliancy

UNIVERSITÉ DU LUXEMBOURG

Anonymisation or pseudonymisation: what to choose?

- Experience has shown that the choice is made case by case and depending on the data set
- Even if in a context of an increasing volume of data and a high risk of re-identification by cross-checking it seems possible the use anonymization techniques for some research projects
- Pseudonymisation is a relevant measure

Conclusion : some words about the luxembourg Law implementing GDPR

- **Scope: Scientific and historical research** purposes**, statistic purpose**
- The controller can derogate to the data subject rights of articles 15,16,18 and 21 of the GDPR if these rights **are likely to render impossible or seriously impair the achievement of the specific purposes**, subject to the implementation of appropriate measures detailed **in article 65**
- **Data subject rights concerned**:
  - Art.15 Right of access
  - Art.16 Right to rectification
  - Art. 18 Right to restriction of processing
  - Art.21 Right to object
  - **The right of erasure is not mentioned**

Luxembourg Law implementing GDPR: conditions of the derogations

- **Criteria(art.65)and accountability:**
  - Taking into account the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons
- **List of mandatory measures.**
- **The controller has to justify each exclusion of the measures detailed**
- **A list of measures provided in article 65**

Questions

- Questions?
- Remarks?