Challenges of GDPR implementation in public research

Chloë Lellinger, Sandrine Munoz and Laurent Prévotat, DPOs

LUXEMBOURG INSTITUTE OF HEALTH
RESEARCH DEDICATED TO LIFE

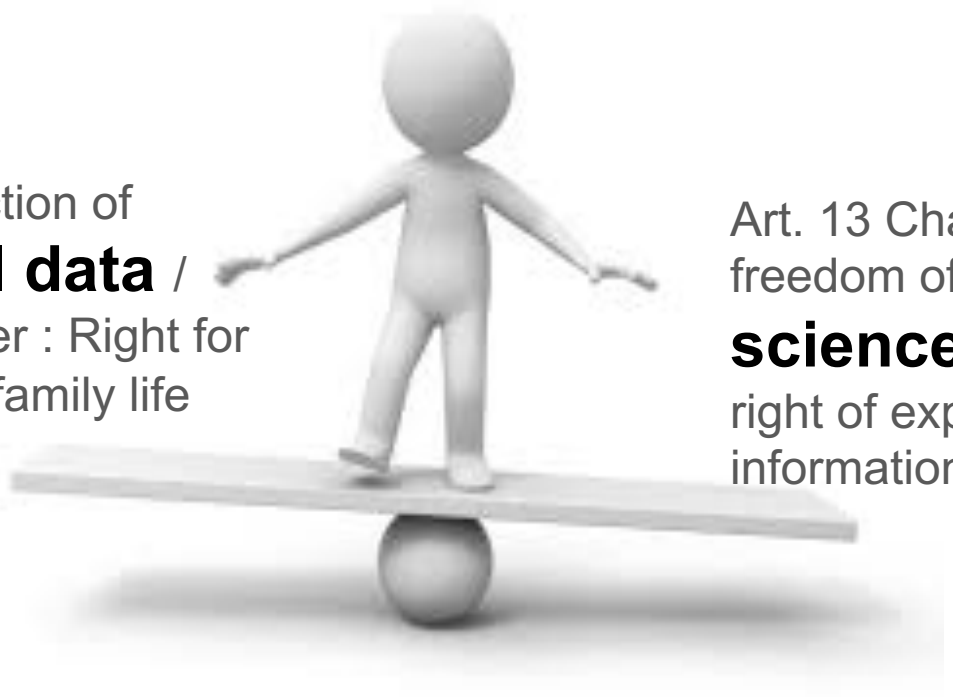
LISER
LUXEMBOURG INSTITUTE OF SOCIO-ECONOMIC RESEARCH

uni.lu
UNIVERSITÉ DU LUXEMBOURG

INTRODUCTION

Data protection in scientific research:
an imbalance between 2 fundamentals rights

Art. 8 protection of **personal data** / Art. 7 Charter : Right for private and family life



Art. 13 Charter of : freedom of the arts and **sciences** / Art. 11 : right of expression and information

INTRODUCTION

- “My feeling is that the biggest challenge we have in this debate is defining what genuine scientific research truly is” G. Buttarelli, EDPS, 5th worldwide congress for freedom of scientific research

- **Systematic activities which increase the stock of understanding and knowledge and their application**

- Act in the context of a public mission recognized by the state (i.e. reflected through public funding or public contracts)

INTRODUCTION

- Scientific research (GDPR), it covers «technological development, fundamental research applied research and privately funded research»

- Specific regime for academic freedom and scientific research set up in the GDPR (art. 85/art. 89) and in the Luxembourg law (art.65/art.66)
  - Legimity to process sensitive catagories of personal data
  - Presumption of purpose compatibility with the purpose for which the data were initially collected
  - Derogations to data subjects rights (only if the exercice of those rights would likely impair the achievement of research purposes)
  - Derogations for some transfer to a non-european country
  - Derogations to Data retention limits, if safeguards in place

What are the main challenges?

- Legal qualification of the parties
- Data Protection Impact Assessment (DPIA)
- Transfer of personal data to third countries
- Further processing for research purposes

Legal qualification of the parties

Controller, joint-controller, processor

Legal qualification of the parties
Issue and challenges

Legal qualification is the **first key point** in terms of obligations and contractual framework

- GDPR clearly mentions **specific obligations** depending on the role of controller or processor of the parties

- GDPR clearly requires specific **agreements/provisions**:
  - The relationship between controller and processor shall be ruled by a contract (**art.28**)
  - Joint-controllers shall determine in a transparent manner their respective responsibilities (**art.26**)

Legal qualification of the parties
Issue and challenges

Do not underestimate data protection aspects in agreements (personal data processing clarifications, time needed…)

In research, legal qualification is complex and source of interpretation:

- Done on a case by case basis in relation with personal data processing carried out by the parties
- Collaborations may often lead to joint-controllership qualification
- Depending on the context, research institutions can be qualified as processors

Legal qualification of the parties
One scenario in research

UNIVERSITÉ DU LUXEMBOURG

Context

- The public research institution **A** wants to lead a scientific research project with a public research institution **B**

- **A** and **B** want to ask the services of a public research institution **C** to collect health data without participation of **C** to the research project

- **A** and **B** decide who will have access to the data and what means of processing will be used

A and **B** may be qualified as joint-controllers and **C** as processor

Legal qualification of the parties
One scenario in research

1. In accordance with art.26 **a data sharing agreement/collaboration agreement** must be concluded between **A** and **B**
2. In accordance with article 28 **a data processing agreement** must be concluded between **A**, **B** and **C**

- **A** and **B** must discuss their collaboration, especially related to data subjects information and rights, records of personal data, personal data breach and Data Protection Impact Assessment where needed
- The definition of dedicated contact points for data protection is recommended
- The determination of personal data processing and tasks allocation of the parties is also important

Data Protection Impact Assessment

DPIA

Data Protection Impact Assessment (DPIA)

DPIA is a **privacy-related** impact assessment whose objective is to identify and analyse how privacy might be affected by certain actions or activities.

CNPD Black list

List of processing operations subject to a DPIA
Processing of genetic data + one or more EDPB criteria, except healthcare professionals delivering health services
Processing of biometric data for the purpose of identifying data subjects + one or more EDPB criteria
Datasets that have been matched or combined from processing operations with different purposes (from the same or from different data controllers) on condition that they produce legal effects or a significant impact on the data subject + one or more EDPB criteria
Systematic and regular monitoring the activity of the employees concerned on condition that it produces legal effects or a significant impact on the data subject
Processing covering personal data about the entire country's population (unless a DPIA has already been carried out as part of the establishment of the legal basis)
Processing for scientific or historical research purposes or archiving purposes in the meaning of art. 63 to 65 of the law of 1 August 2018
Systematic geolocation of data subjects
Indirect data collection + one or more EDPB criteria

What is a Privacy risk?

UNIVERSITÉ DU LUXEMBOURG

Risk impacting the rights and freedoms of individuals

- Information about you used without your knowledge or permission (unreasonable/**unfair uses of your information**)
- Reputational/financial damages from unauthorized **disclosure of** a person's psychological or **medical condition** or social activities could lead eg. to job loss
- Unauthorized disclosure of personal information **can expose people to harassment** and surveillance from stalkers
- **Intrusion into people's private** lives (the installation of spyware on computers that enable the recording of users engaged in private activities)

What are the categories of risks to manage?

Risks that can lead to:

- an **illegitimate access** to personal data
- **unwanted modification** of personal data
- **disappearance** of personal data

To determine the appropriate technical and organizational **controls to protect personal data**

Different methodologies to propose an objective analysis of the risk

UNIVERSITÉ DU LUXEMBOURG

One of the first challenge: To choose the DPIA methodology

- **ENISA** “Recommendations for a methodology of the assessment of severity of personal data breaches”
- **CNIL** “Methodology for Privacy risk management. How to implement the Data Protection Act”

Risk matrix

Impact \ Likelyhood	1	2	3	4
4	4	8	12	16
3	3	6	9	12
2	2	4	6	8
1	1	2	3	4

Next challenge: To set-up a process and build your tool

Who contribute to the DPIA?

other challenge: who is involve?

- Point of Contact
- Risk Manager
- Processing owner (group leader)

- DPO

Principle and Use case

1. Risk : Unwanted modifications to data in the study database (aim: personalized treatment)

2. 1st Assessment **w/o mitigation:**

Applicable?	Gross Impact	Gross Likelihood	Gross Risk Value	Risk Status without existing controls
Yes	Maximum	Possible	12	To be improved

3. Mitigation measures: Training, Access rights management, input mask, monitoring

4. 2nd Assessment **with mitigation:**

Impact	Likelihood	Net Risk Value	Risk Status	Action
Maximum	Unlikely	6	Acceptable	No action required

If the residual risk is **too high** → CNPD notification

DPIA aims to help the organization
to protect the Individuals from harm generated
by the collection, dissemination, or use of personal data

Transfer of personal data to third countries

Outside EU and EEA

Transfer of personal data to third countries

- Personal data cannot be shared without an appropriate contractual framework

- Research institutions aim to perform projects with partners all around the world

- Research collaborations can involve transfer of personal data to research institutions located outside EEA and EU

- GDPR contains specific provisions about transfer of personal data outside EU and EEA: implementation of appropriate safeguards is required

  ➡ In case of an adequacy decision with a country the transfer is authorised **if the adequacy decision also aims research and academic sector (most of the time)**

https://cnpd.public.lu/en/dossiers-thematiques/transferts-internationaux-donnees-personnelles/Reglement-general-sur-la-protection-des-donnees.html

Transfer of personal data to third countries
Focus on the UK

UNIVERSITÉ DU LUXEMBOURG

In case of collaboration involving research institutions in the UK

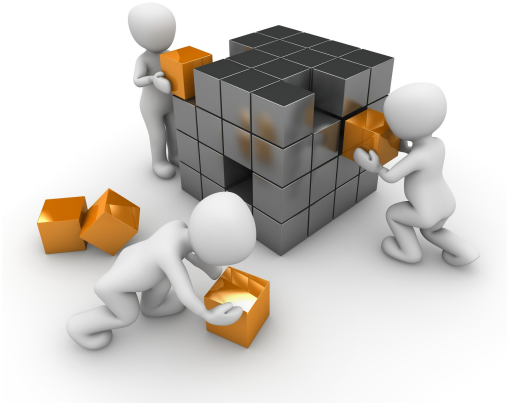
- Following the signature of the withdrawal agreement **(BREXIT) UK** is not considered as a third country until **31st December 2020**
- **UK will continue to apply GDPR until 31st December 2020**
- At the same time an adequacy decision is expected to take over after 31st of December 2020

Transfer of personal data to third countries

- Without any adequacy decision, an appropriate safeguard must be implemented

- Most of the time, **standard contractual clauses** are concluded

- For example, a research institution A in Europe wants to lead a research project with an institution B located in Australia
  - Collection of personal data will be done in Europe and in Australia
  - Sharing of personal data will occur in both side



Transfer of personal data to third countries

- EC Standard contractual clauses must be concluded between the research institution A in Europe (exporter) and the research institution B in Australia (importer)

- Standard contractual clauses are used as appropriate safeguards, however they are:
  - Not fully adapted to research
  - Source of negociation between the partners

➡ A revision of the EC Standard contractual clauses is expected in 2020

➡ An alternative: asking explicit consent of data subject (derogation under specific conditions)

Further processing for scientific research purposes

Derogation to the purpose limitation principle

UNIVERSITÉ DU LUXEMBOURG

Derogation to the purpose limitation principle

- Researcher can go beyond the purposes for which they first collected (so long as the data will only be used for that purpose)

- Art. 5 b) GDPR « Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further for (…) scientific or historical research purposes or statistical purposes shall be in accordance with art. 89(1), not be considered to be incompatible with the initial purposes.»

- + Legal basis
  - Consent
  - Public interest

Derogation to the purpose limitation principle

- Rec. 50 GDPR « Further processing for (…) scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.»

- Rec. 50 GDPR « If the processing is necessary for the performance of a task carried out in a public interest (…) Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded for which the further processing should be regarded as compatible and lawful. (…) The legal basis provided by Union or a Member State law for the processing of personal data may also provide a legal basis for further processing.»

Derogation to the purpose limitation principle

How to justify the presumption of compatibility for further processing for research purposes?

- Technical and organisational measures to respect data minimisation (Art. 89 GDPR/65 Lux. law specific regime)
  - Data management plan
  - Encryption
  - Use of privacy enhanced technologies
  - User authentification and traceability
  - Anonymisation or pseudonymisation «provided that those purposes can be fulfilled in that manner» (art. 89 §1 GDPR)
- Public funding for the research project (?)
- Ethical approval (?)
- Others to be discussed ?

Thoughts

"GDPR is not there to act as a barrier to research, nor to impede it. We are in fact heading to protect the same human being."

G. Buttarelli, EDPS,

5th world congress for freedom of scientific research

Stay connected with us!