LNDS

Ensuring Compliance: Data Protection Laws and Risk Assessment in Research

When and how to carry out a DPIA

Francesco Vigna, PhD, DPO, CIPM

Data Privacy Day 2025 - Maison du Savoir, Esch-Sur-Alzette

28th January 2025

1. “Risk based approach” and its inclusion into data protection law compliance

2. Processing personal data for “research” purposes

3. How to organize the DPIA process and quick wins

The approach

A mixed right/risk-based approach in GDPR

LNDS

Risk based approach in data protection law

How risk is embedded into GDPR

- Article 5(2) & 24
- Article 25 GDPR DP by design and by default
- Article 32 security of the processing activities
- Article 35 Data protection impact assessment

Risks for data subjects

- Privacy assessment
- Privacy impact assessment

Risks for the organization

Risk based approach in data protection law

How risk is embedded into GDPR

- Article 5(2) & 24
- Article 25 GDPR DP by design and by default
- Article 32 security of the processing activities
- Article 35 Data protection impact assessment

Risks for data subjects

- *Data transfer impact assessment*
- *Legitimate interest impact assessment*
- *Re-identification risk assessment*
- *Vendor assessment*

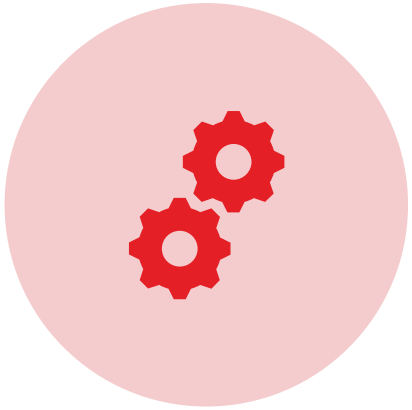
- Privacy assessment
- Privacy impact assessment

Risks for the organization

Rights based vs risk-based approach

A mixed approach

RIGHTS BASED APPROACH: TRADITIONAL LEGAL APPROACH FOLLOWING A BINARY LOGIC (COMPLIANCE VS NOT COMPLIANCE)



RISK BASED APPROACH: GRANULAR, SCALABLE LOGIC - HOW MUCH RISK IS EMBEDDED INTO PROCESSING OPERATIONS, AND WHAT MEASURES TO ADOPT TO REDUCE THE RISK

CORE PRINCIPLES OF GDPR ARE STILL RIGHT-BASED, RISK-BASED APPROACH APPLIES TO COMPLIANCE OBLIGATIONS, SUCH AS ACCOUNTABILITY, DPIA, ETC.

Risk based approach in data protection law

How to systematically implement GDPR compliance?

System of policies and procedures:

- Privacy policy
- Procedure for managing data subject rights
- Procedure for embedding privacy consideration into the design of product, services and processes
- Procedure to decide when and how to carry out a DPIA
- Etc.

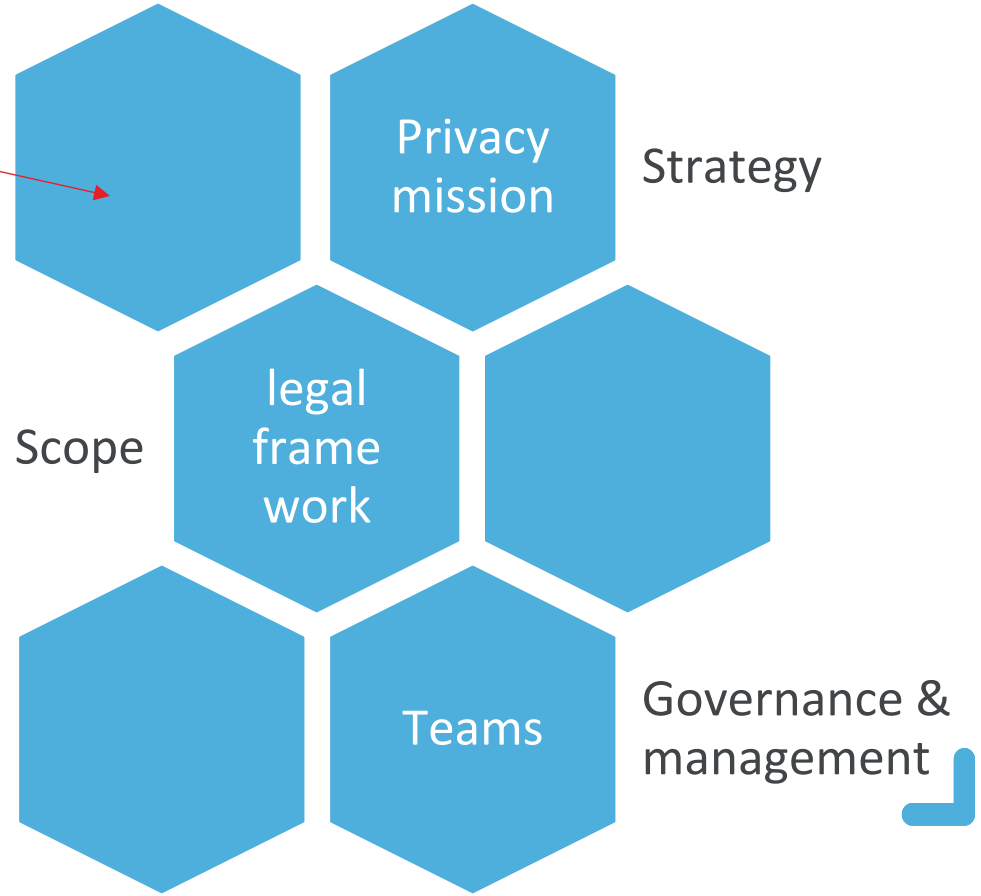
Risk based approach in data protection law

How to systematically implement GDPR compliance?

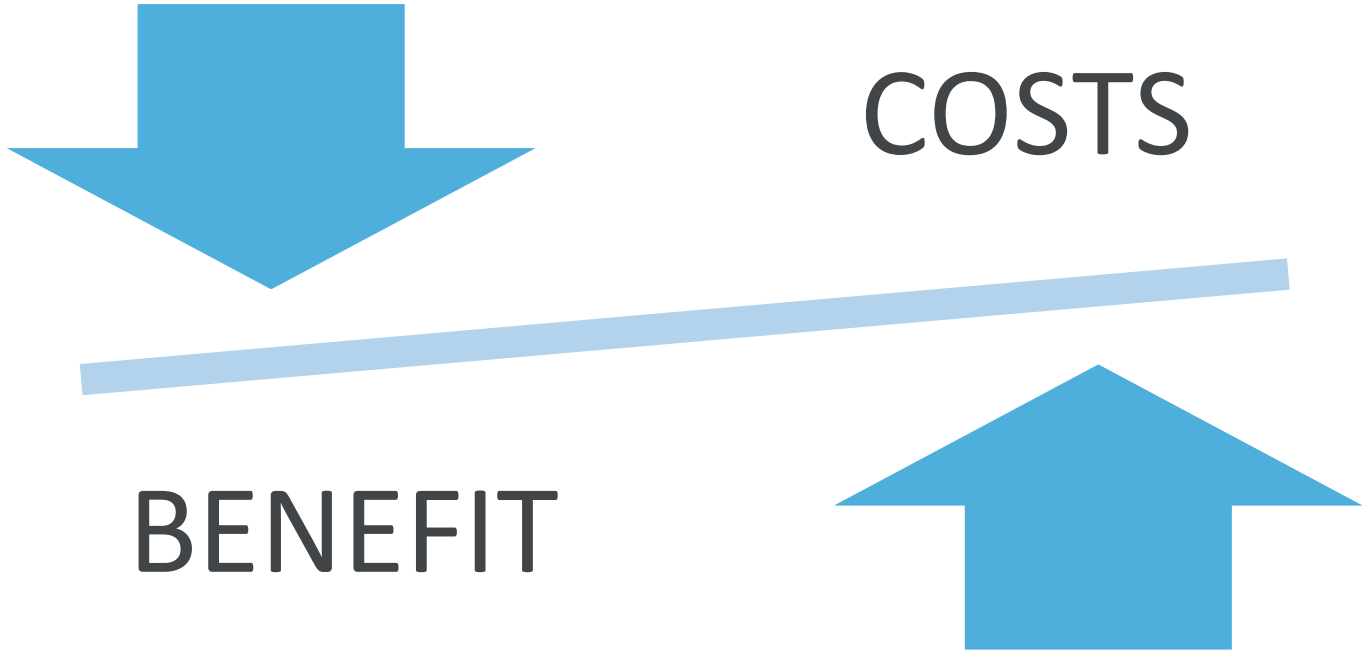
System of policies and procedures:

- Privacy policy
- Procedure for managing data subject rights
- Procedure for embedding privacy consideration into the design of product, services and processes
- Procedure to decide when and how to carry out a DPIA
- Etc.

Privacy management system



Compliance costs



Example

Costs of data breaches

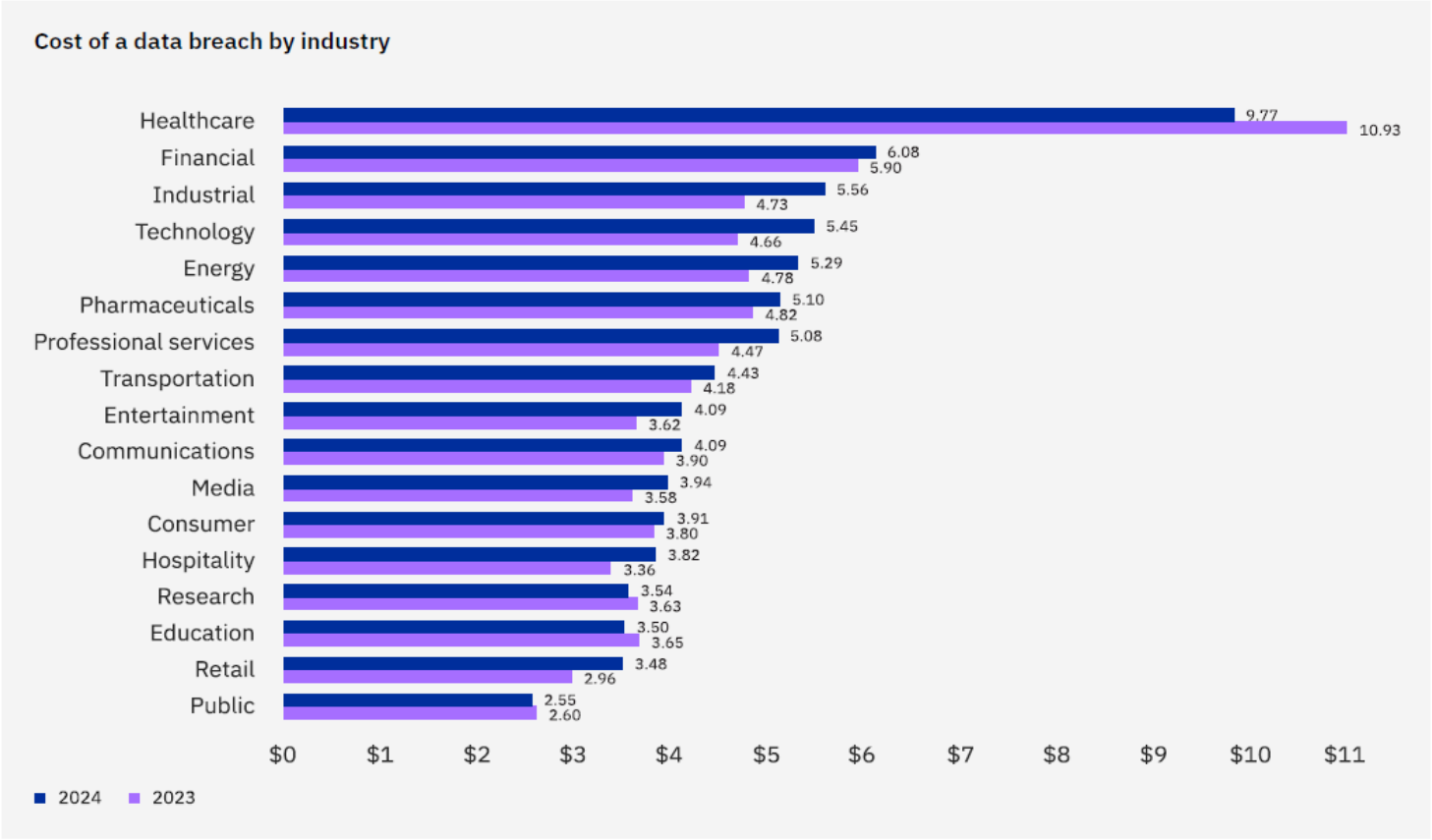


Figure 3. Measured in USD millions

IBM, Ponemon Institute, Cost of a Data Breach, Report 2024

Cost of a data breach by country or region

#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Example: cost of data breaches

Quick wins:

- Training and awareness
  - Posters, newsletters, periodic “knowledge sharing” events
  - Training already embedded in the onboarding procedure
- Data protection by design processes

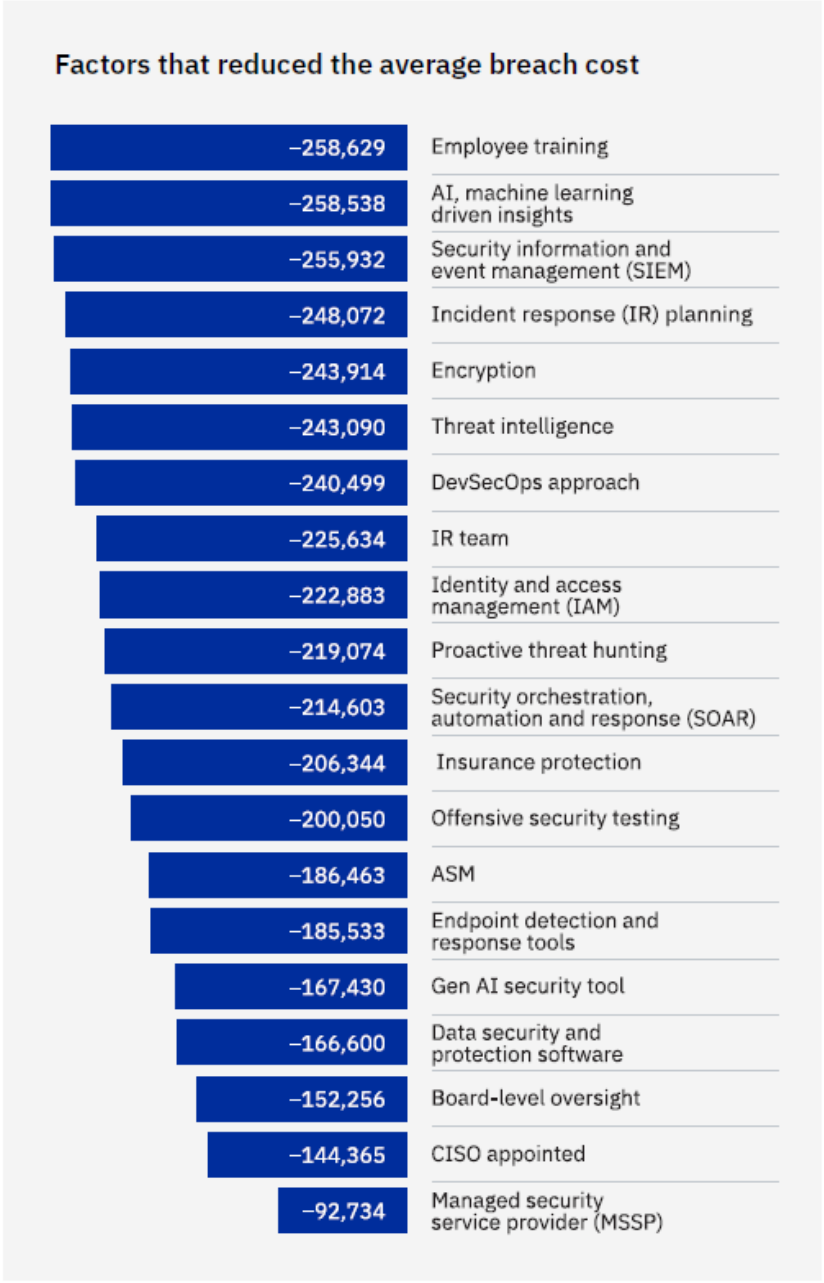


Figure 25. Cost difference from USD 4.88M breach average; measured in USD

IBM, Ponemon Institute, Cost of a Data Breach. Report 2024

The processing of personal data for scientific research

A special regime under the GDPR

LNDS

Processing of personal data for research

Concept of scientific research in data protection law

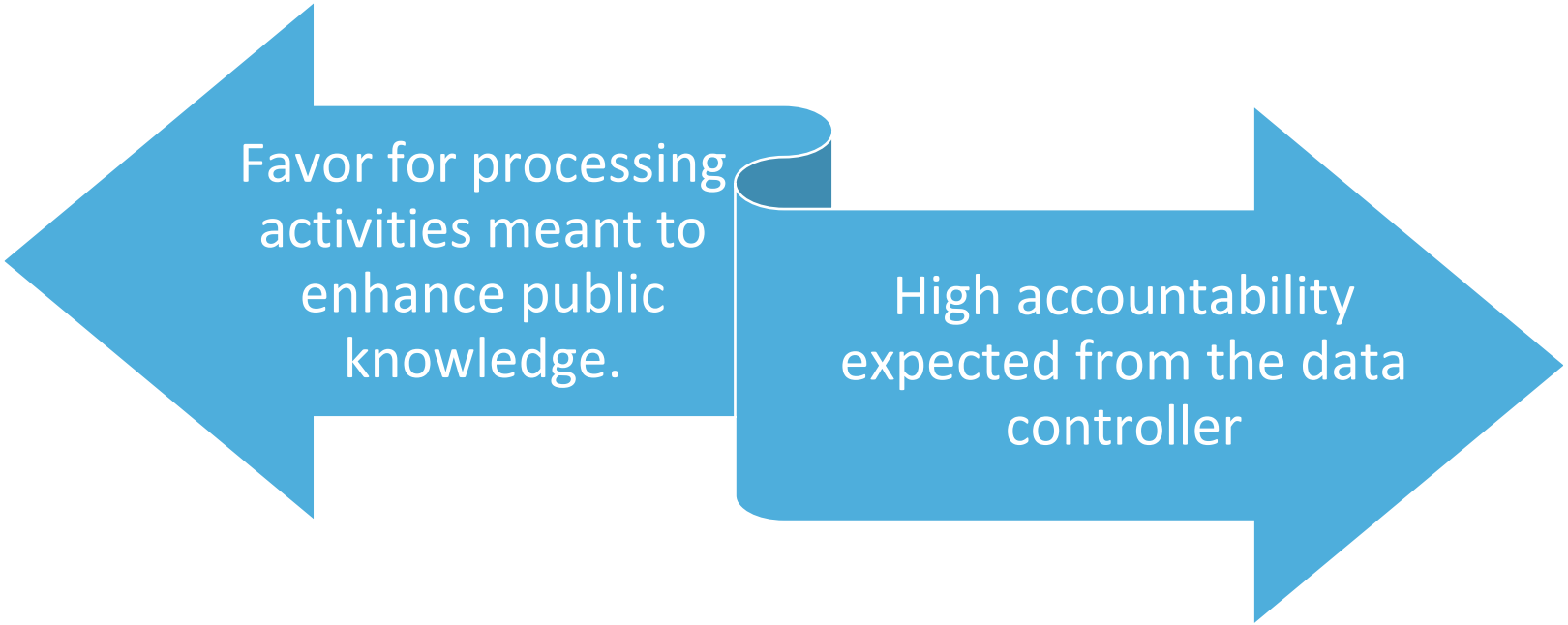
Recital 159 GDPR: "[…] scientific research purposes should be interpreted in a broad manner broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. [...] . Scientific research purposes should also include studies conducted in the public interest in the area of public health."

Preliminary opinion on data protection and scientific research EDPS

- "not only academic researchers but also not-for-profit organisations, governmental institutions or profit-seeking commercial companies can carry out scientific research."
- For a controller to simply claim to process data for the purposes of scientific research is not sufficient, instead:
  - relevant sectoral standards of methodology and ethics apply, including the notion of informed consent, accountability and oversight;
  - the research is carried out with the aim of growing society's collective knowledge and wellbeing, as opposed to serving primarily one or several private interests

Processing of personal data for research

In general, in the GDPR:



Special regime for scientific research

The favor for scientific research purposes

- Dedicated legal basis (where applicable)
- Potential exceptions from some obligations for the data controller
- Further processing deemed compatible (where applicable)
- Possibility for member states to integrate the GDPR with national law

Responsibility for the data controller

Accountability

Article 89 GDPR is pivotal (which covers also archiving purposes in the public interest, historical research purposes or statistical purposes)

- Par (1) – appropriate technical and organizational safeguards (such as data minimization or pseudonymization)
- Par (2) – MS laws can impose derogations to certain rights, as long as the safeguards in par (1) are respected and the fulfillment of such rights are likely to seriously impair or render impossible the purpose of scientific research

Articles 63-65 Act of 1st of August 2018

- In order to benefit of exemptions or relying on certain legal basis appropriate safeguards shall be implemented.

Special regime for scientific research

Understand your need to carry out a DPIA

- **Article 89 GDPR & Articles 62-65 Act of 1st of August 2018**
  - "the performance of an impact assessment of the planned processing activities on the protection of personal data is a measure" is one of the appropriate measures.
- **Article 35.4 GDPR lists – CNPD deliberation n. 34/2019**
  - scientific research falls under the list of processing activities that requires a DPIA mandatorily
- **Article 35.3 GDPR requirements**
  - automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
  - processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;
  - systematic monitoring of a publicly accessible area on a large scale.
- **WP29 WP248 guidelines on data protection impact assessment**
  - Set of 9 criteria to understand the need for a DPIA
  - In general, if at least 2 criteria are met, then DPIA is necessary

Need for the DPIA

Summary of elements might trigger the duty for a DPIA

Type of processing	Reference
Automated decision making, evaluation and scoring, or systematic monitoring, innovative use of technologies	GDPR art. 35, WP248
Processing on a large scale	GDPR art. 35, WP248
Monitoring of public area	GDPR art. 35
Genetic or biometric, or other sensitive data	CNPD, WP248
Combination and matching from different sources	CNPD, WP248
Employees monitoring, or data concerning vulnerable data subjects	CNPD, WP248
Processing on the whole national population	CNPD
Scientific, historical and statistical purpose	CNPD
Geolocation	CNPD
Impossibility to provide information	CNPD
Processing that prevent data subjects from exercising rights or similar effects	WP248

How to carry out a DPIA

Practical consideration for carrying out a DPIA

LNDS

When?

At what moment of the data life cycle to carry out a DPIA

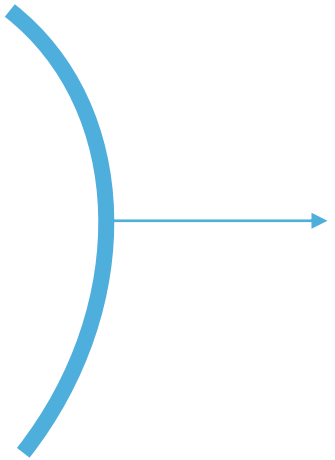
1) During the ideation of a project
2) In case of changes in the processing activities, i.e., new potential risks

Carrying out a DPIA

Content of the DPIA

Art. 35.7 GDPR

- description of the envisaged processing operations and the purposes of the processing;
- an assessment of the necessity and proportionality;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks
- Collecting the view of data subjects



- Risk identification
- Risk analysis
- Risk evaluation
- Risk treatment

A. Necessity and proportionality is the first step, if not satisfied there should be no processing at all
B. Not an assessment simply meant to put on the same level the cost and benefit stemming from the data processing, but it should rather be an assessment meant to mitigate the risks for the data subjects' fundamental rights.

Carrying out a DPIA

How to organize a DPIA

- Having a process that support the organization understanding when and if a DPIA must be carried out
- Understand the stakeholders you need to involve
  - Process owner (e.g., researchers)
  - ELSI experts
  - Data stewards, IT expert, security expert, risk management, lawyers
  - Leadership
  - DPO
- Assign roles and responsibilities, such as using a RACI matrix (Responsible, Accountable, Consulted, Informed)
- Establish timeframes for the DPIA performance and for its review
- Train the organization on the performance of the DPIA procedure.

Carrying out a DPIA

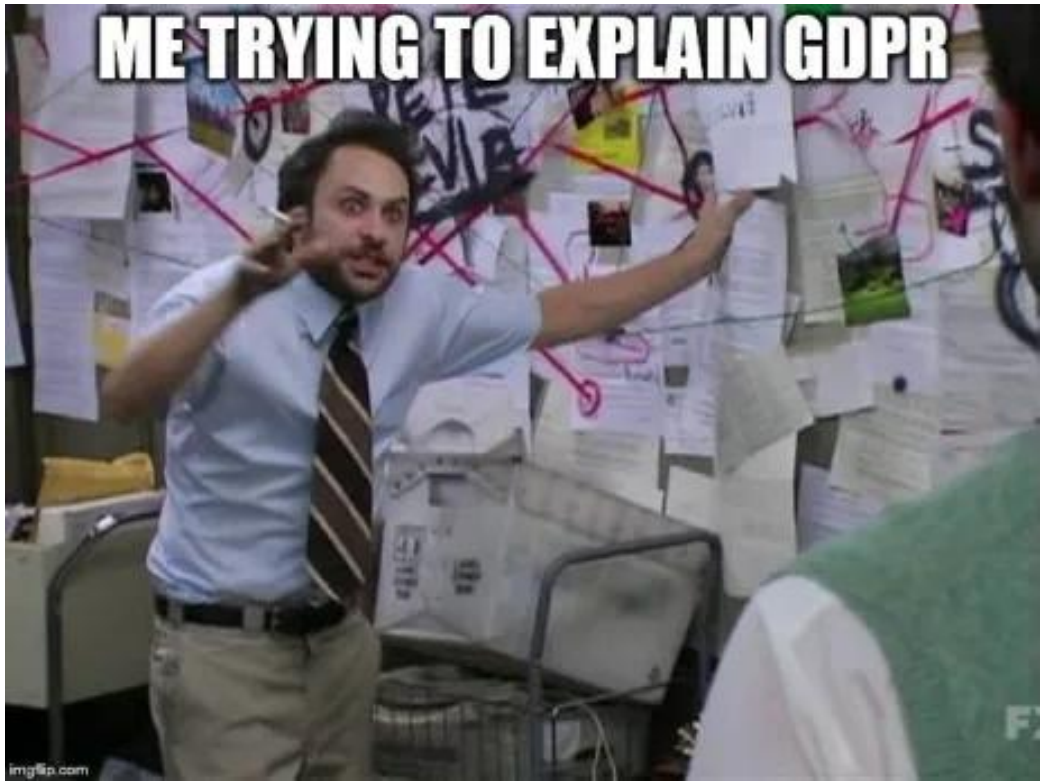
What methodology?

Essential steps to follow in a DPIA:

- Explaining the need for a DPIA
- Description of the data processing activities, context and purposes
- Data flows description and assets involved, presence of processors, transfer of data to third countries
- Explain the result of the consultation with data subjects or why it was not possible/necessary to do it
- Assessment of the respect of GDPR principles & data subjects' rights
  - Measures already envisaged to comply with these principles and rights
- Assessment of the risks in case of violation of confidentiality, availability, integrity
- Risk treatment
- Conclusion, validation and review

Conclusion

Data protection requirements can be cumbersome, especially in research context.



Conclusion

Quick wins

- Invest time in training and awareness
- Having policies and procedure that clearly identifies roles and responsibilities
- Create a process to embed DP assessment since the outset of project and processing. A good DP by design and default approach reduces a lot the efforts during the DPIA

References

- R. Gellert, Understanding the notion of risk in the General Data Protection Regulation, January 2018, Computer Law & Security Review 34(2), DOI:10.1016/j.clsr.2017.12.003
- IBM and Ponemon Institute, Cost of a Data Breach report 2024
- Working party article 29, WP248 Guidelines Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679
- Délibération 34/2019 du 6 mars 2019 de la Commission nationale pour la protection des données portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise

CONTACT US !

www.lnds.lu

+352 621147573

info@lnds.lu

6, Avenue des Hauts-Forneaux

L-4362 Esch-sur-Alzette

LNDS

LUXEMBOURG NATIONAL DATA SERVICE