Data management plan and research with personal data

DANAJA FABČIČ POVŠE
Vrije Universiteit Brussel (VUB)
Research Group on Law, Science, Technology & Society (LSTS)
Health and Ageing Law Lab (HALL)

University of Maribor Open Science Summer School
Maribor, Slovenia
September 2022

Agenda

1. FAIR data & Commission-funded projects
2. GDPR 101
3. Commission's research ethics
4. New proposals – EU HDS and DGA
5. Exercises

FAIR data

Opening up research data in EU funded projects

Source of funding for your research project?

2014-2020
80 billion EUR

2021-2027
95 billion EUR

Horizon Europe: structure

Pillar I

Excellent Science

European Research Council

Marie Sklodowska-Curie Actions

Research Infrastructures

Pillar II

Global Challenges and European Industrial Competitiveness

Clusters

- Health
- Culture, Creativity and Inclusive Society
- Civil Security for Society
- Digital, Industry and Space
- Climate, Energy and Mobility
- Food, Bioeconomy, Natural Resources, Agriculture and Environment

Non-nuclear direct actions of the Joint Research Centre

Pillar III

Innovative Europe

European Innovation Council

European Innovation Ecosystems

European Institute of Innovation and Technology

Source of funding for your research project?

Some funders require sharing data…

- EU – Horizon 2020 and Horizon Europe: Open data research pilot (ORD)
- US – from 2026 for projects funded by public agencies (link)
- Must make research data FAIR:
  - Findable
  - Accessible
  - Interoperable
  - Re-usable

FAIR data

- Create a data management plan:
  - The handling of research data during and after the end of the project,
  - What data will be collected, processed and/or generated,
  - Which methodology and standards will be applied,
  - Whether data will be shared/made open access,
  - How data will be curated and preserved (including after the end of the project),
  - Etc.

Data protection questions

Whose data?

What can you learn about a specific person?

How easy would it be to identify an individual?

- no specific provisions in the Open Data Research Pilot requiring the participants to anonymise data

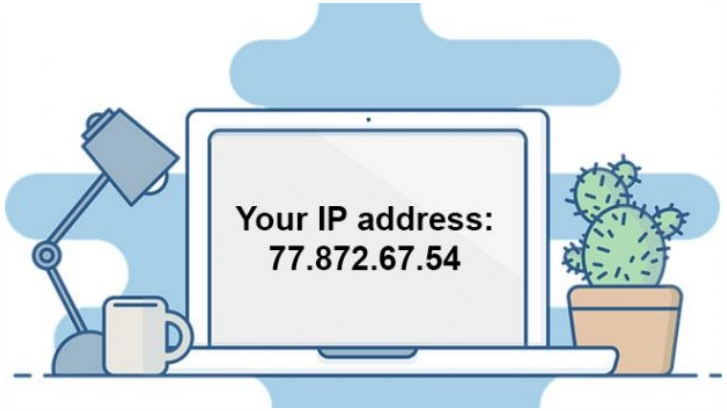
What is personal data?

> (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- Personal data
  - (1) any information (2) relating (3) to an identified or identifiable (4) natural person (4 elements)
  - Only *anonymous* data falls *outside* GDPR; pseudonymous data is *within* the scope (although enjoying less stringent restrictions)
- Processing

> (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Example: are those personal data?



(source: Article 29 Working Party, Opinion on the concept of personal data; case Breyer C-582/14)

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

HALL health & ageing law lab

TeNDER

Personal data

- Personal data is defined very widely
- Contextual – refers to an individual
- The individual must be IDENTIFIED or IDENTIFIABLE
  - Identifiable from the same dataset or data you are handling, or by other means?
  - See next slide

Personal data

- Definition can unexpectedly cover datasets you don’t expect it to
- CJEU – Breyer case (C-582/14)
  - Dynamic IP = personal data
  - As long as the necessary piece of info to identify the person is available to someone out there…
- In case of doubt, play it safe → safeguards, ethics plan

GDPR 101

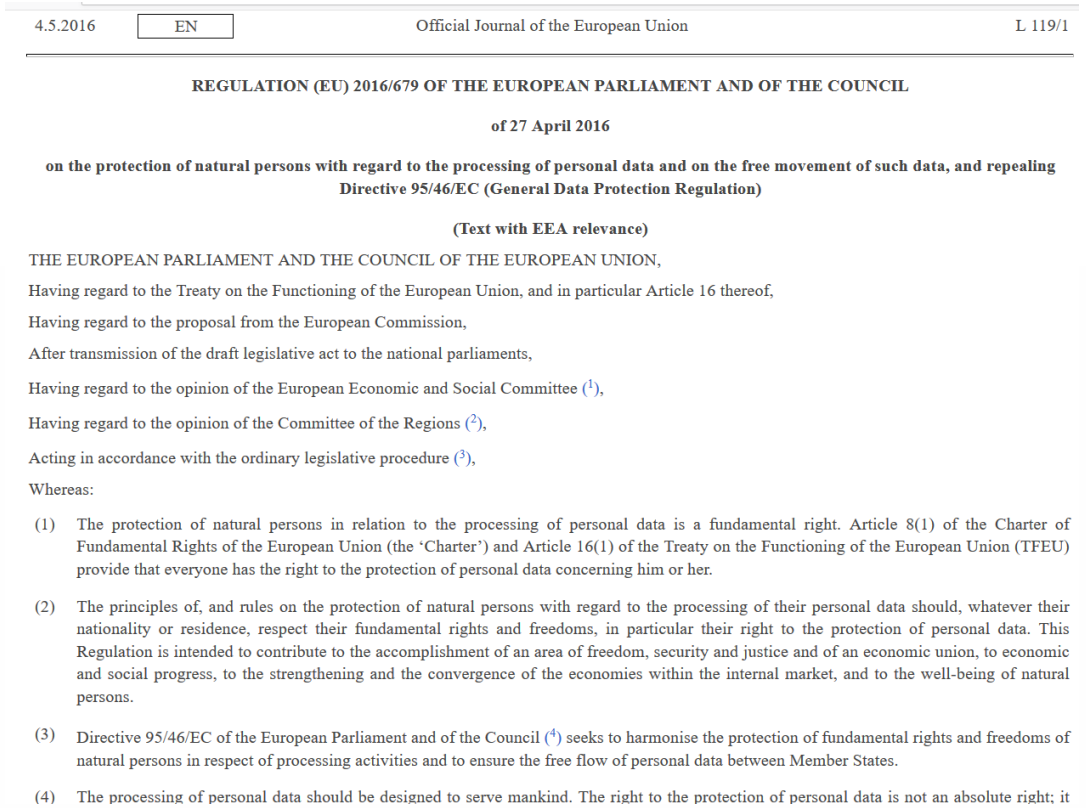
A short-ish introduction

What is the GDPR?

- **G**eneral
- **D**ata
- **P**rotection
- **R**egulation

- Regulation (a type of law) on EU level, applicable from May 25 2018

- Replaces the Data Protection Directive 95/46/EC (and national law)



4.5.2016 EN Official Journal of the European Union L 119/1

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 April 2016

on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ([1]),

Having regard to the opinion of the Committee of the Regions ([2]),

Acting in accordance with the ordinary legislative procedure ([3]),

Whereas:

(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

(3) Directive 95/46/EC of the European Parliament and of the Council ([4]) seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

(4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

HALL health & ageing law lab

TeNDER

What is the GDPR?

- Data protection – mitigating risks to **human rights**

  e.g. PRIVACY, FREEDOM OF EXPRESSION, NON-DISCRIMINATION

Dutch childcare benefit scandal an urgent wake-up call to ban racist algorithms

The Dutch government risks exacerbating racial discrimination through the continued use of unregulated algorithms in the public sector, Amnesty International said in a damning new analysis of the country's childcare benefit scandal.

The report ***Xenophobic Machines*** exposes how racial profiling was baked into the design of the algorithmic system used to determine whether claims for childcare benefit were flagged as incorrect and potentially fraudulent. Tens of thousands of parents and caregivers from mostly low-income families were falsely accused of fraud by the Dutch tax authorities as a result, with people from ethnic minorities disproportionately impacted. While the scandal brought down the Dutch government in January, sufficient lessons have not been learnt despite multiple investigations.

My Experiment Opting Out of Big Data Made Me Look Like a Criminal

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

HALL health & ageing law lab

TeNDER

GDPR: scope of application

Personal data (rept.)

> (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- Personal data
  - (1) any information (2) relating (3) to an identified or identifiable (4) natural person (4 elements)
  - Only *anonymous* data falls *outside* GDPR; pseudonymous data is *within* the scope (although enjoying less stringent restrictions)
- Processing

> (2) 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Sensitive personal data

Article 9

Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

- But you can escape this prohibition if:

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(e) processing relates to personal data which are manifestly made public by the data subject;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Sensitive personal data – contd.

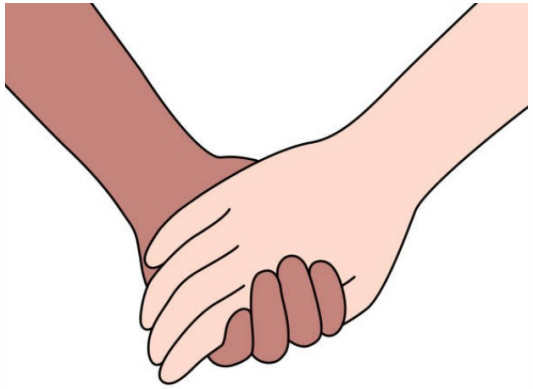
- Art. 4 (13) **'genetic data'** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
- Art. 4 (14) **'biometric data'** means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
- Art. 4 (15) **'data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Sensitive personal data – contd.

- Trend to widening the definition
  - CJEU case ***Vyriausioji tarnybinės etikos komisija*** (C-184/20):
  - personal data that indirectly disclose the sexual orientation of a natural person constitutes processing of special categories of personal data

- But photos are on principle not sensitive unless combined with facial recognition/biometrics … (EDPS)

- What now? → check specific rules of your funder/university for guidance on how to treat sensitive PD



Roles and responsibilities

Data controller

Art. 4(7)

Determines the purposes and means of the processing = **why and how data are processed**

Data processor

Art 4.(8)

Processes data on behalf of the controller

Examples: payment service provider, cloud service provider

EITHER-OR (mutually exclusive roles)

➔ controller-processor agreement (binding contract!)

Responsibility for compliance

- We don’t have “official” confirmation from the court yet if researchers are controllers (but the university as the employer/institution probably is)
  - Pick your processor with care! (= the software or tools you will be using in your research)

Why should we care about processors?

- The thorny issue of using Google products
- Google – a recent Danish decision (***Østre Landsret***) that if you store **children's data** on **Google products** (Docs, Drive, Forms…) it is not compatible with the GDPR, **unless you encrypt** the data (a pending CJEU case, but no info available yet)

- This means risking a fine + must stop processing or delete the data…
  - Ask your university's ethical committee (or DPO or DMP people)
  - Find alternatives? EUSurvey?
  - Check privacy policies

Specific rules on DP in research

Article 89

Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

Caveat – specific rules, applicable to research activities, are not unified on EU level and will depend on the country your research is performed in!

https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/

Specific rules on DP in research

- What is scientific research in GDPR context?
- No definitions, but it includes (Recital 159)
  - technological development and demonstration
  - fundamental research
  - applied research and privately funded research
  - studies conducted in the public interest in the area of public health

- Consequences for:
  - Legal grounds
  - Compatible further processing (reuse of data)

Principles and obligations

Data quality principles

Lawfulness, fairness and transparency

Purpose specification

Data minimization

Data accuracy

Storage limitation

Data integrity and confidentiality

Data quality principles

Lawful, fair & transparent processing

- data processed lawfully, fairly and in a transparent manner vis-à-vis data subject
  - need to find LEGAL BASIS for data processing
  - data subject to understand WHY, HOW and WHICH data are being processed

Data quality principles

Purpose limitation

- collect data for ONE PURPOSE only → for a new purpose: need new legal grounds, for example you need to ask consent again
- if research → can re-use data for a different purpose
- example: analysing PD to assess company security (SVA) → cannot sell data to advertisers of security products

Data quality principles

Data minimization

- ‘adequate, relevant and limited to what is necessary’
- key question: can you achieve the goal without a particular dataset?
- e.g. decrypt only what is necessary, not the whole dataset

Data quality principles

Data accuracy

- data must be correct & up to date
- right to rectification → if inaccurate data, data subject can ask for correction

Storage limitation

- after the data are no longer needed → delete or anonymise

Data quality principles

Integrity and confidentiality

- Keep data secure against:
  - Unauthorised/unlawful processing (external AND internal)
  - Accidental loss, destruction or damage

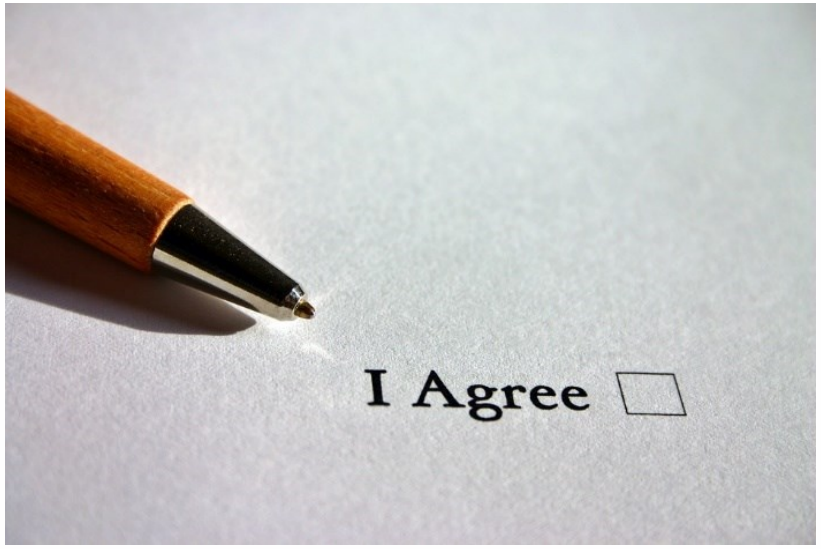
Lawful processing: legal grounds

- Principle of lawful data processing (art. 5(1)(a) of the GDPR)

- Need to find a good **legal basis**. i.e. finding a legal argument that says:
  - 'yes you may process these data'

Lawful processing: legal grounds

- Several available → choose ONE
  - Consent: freely given, specific, informed, unambiguous (art.7-8)
  - Contract
  - Legal obligation
  - Protect vital interest of data subject
  - Task in public interest
  - Legitimate interest



Strict requirements for consent

- Consent (Art. 7, Art. 8 (children))
- Conditions for consent
  - Given freely and be a specific, informed and explicit indication of the data subject's wishes:
    - unambiguous and actively given (**NO pre-ticked boxes**)
    - using clear and plain language = **no legalese**
    - **as easily revoked as given** (click to subscribe, click to opt-out)
  - Granularity → one consent per one specific service
  - Burden of proof: controller to prove all of the above

Strict requirements for consent

- Are you dealing with **children's data**?
  - Persons **under 16 years old** unless national law says otherwise
  - Must obtain **parental authorisation**

Article 8: Conditions applicable to child's consent in relation to information society services

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Reuse of data

- Using data from already existing databases or datasets – new consent or not?

- Confusing legal situation…
  - GDPR: no need for new legal grounds if data is reused for scientific research
  - EDPS opinion (EU's main data protection body): reusing data requires a new legal basis, even if done so for scientific research
  - Funders/ethics boards: please provide consent

- Play it safe, waste time??????

Lalova-Spinks, T., De Sutter, E., Valcke, P., Kindt, E., Lejeune, S., Negrouk, A.,Verhenneman, G., Derèze, JJ, Storme, R/, Borry, P., Meszaros, J., Huys, I. *Challenges related to data protection in clinical research before and during the COVID-19 pandemic: an exploratory study*, manuscript submitted to Frontiers in Medicine, 2022

Reuse of data – provisions in the GDPR

Art. 5(2):

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 processing for archiving purposes in the public interest, **scientific or historical research purposes** or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘**purpose limitation**’);

Art. 89(1)

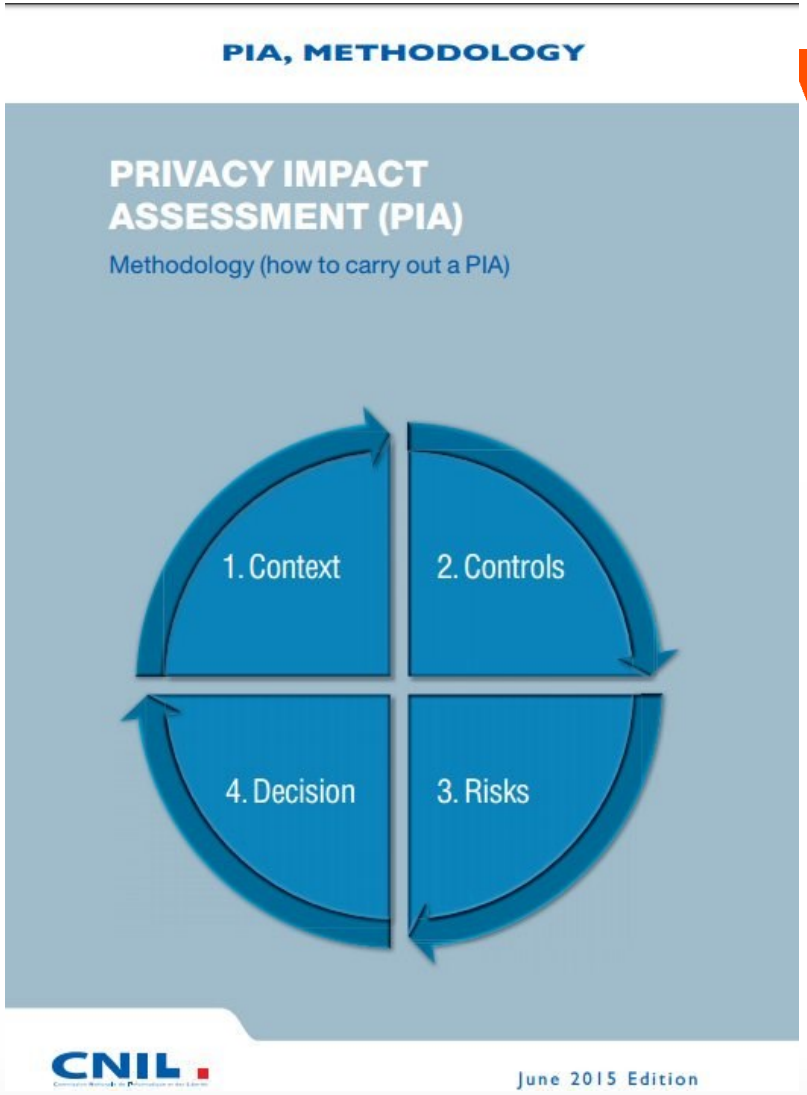
Processing for archiving purposes in the public interest, scientific or historical **research purposes** or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by **further processing which does not permit or no longer permits the identification of data subjects**, those purposes shall be fulfilled in that manner.

Safeguards

Data protection impact assessment

= DPIA

- A useful tool to identify, assess and manage **RISKS** to **individuals' rights**: privacy, freedom of expression, dignity …
- Demonstrates effort to comply
- Existing tools!
  - CNIL DPIA (free, OS, app available)
  - ECPC – UMaas (short&sweet, targeted to companies)
  - EDPB opinions (collection of approved methodologies)



Data protection impact assessment

- When is it obligatory?
  - Excellent questionnaire on p. 5:
  - https://edps.europa.eu/data-protection/our-work/publications/guidelines/data-protection-impact-assessment-list_en

  - Conditions in art. 35 of the GDPR:

Where a type of processing in particular **using new technologies**, and taking into account **the nature, scope, context and purposes of the processing**, is likely to result in a **high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

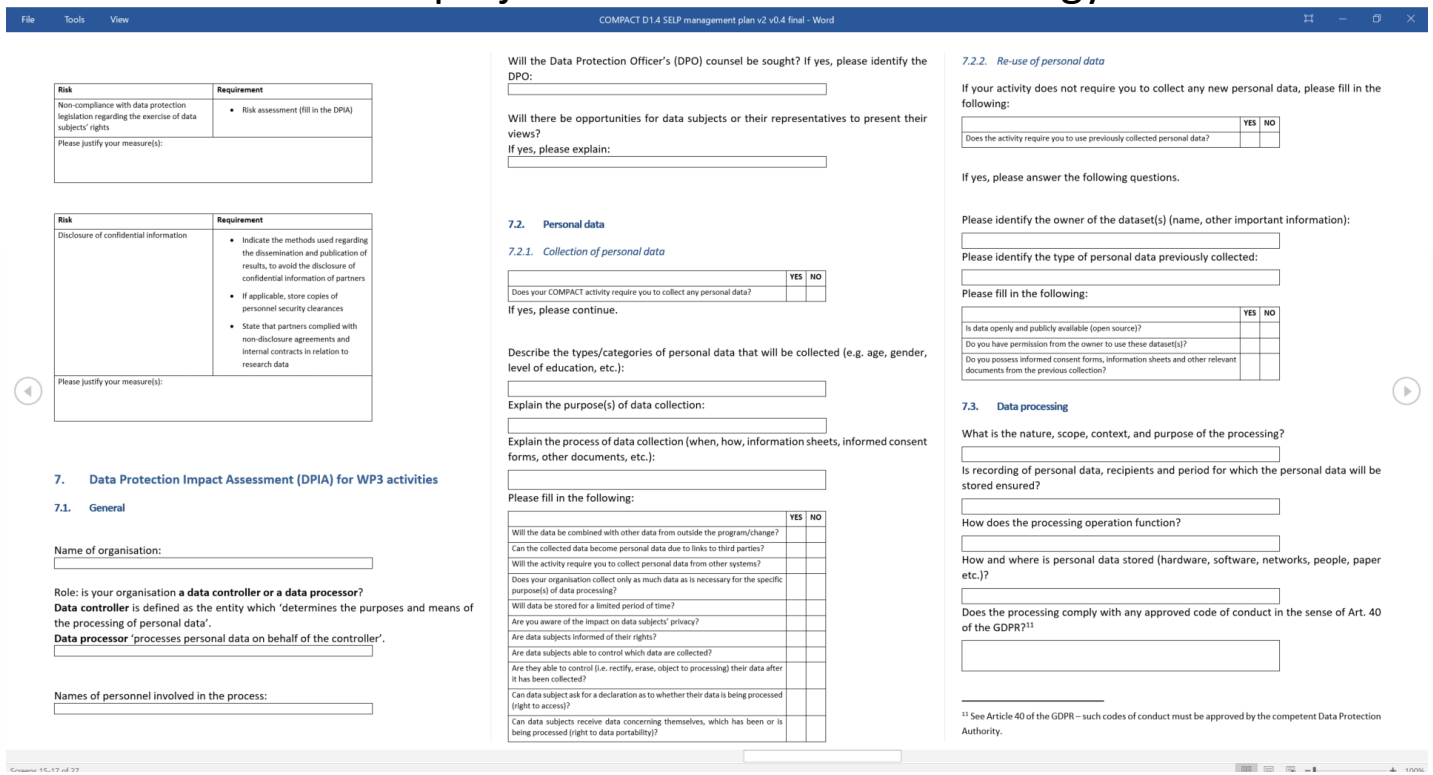
Data protection impact assessment

- Often required for research projects rather than a specific research activity
- DPIA rarely a part of a PhD project
- In doubt, consult internal university policy or ethics committees (if existing)

Added value? Address wider societal or ethical implications of research!

An example of a DPIA

DPIA for the COMPACT project: Commission methodology



File Tools View — COMPACT D1.4 SELP management plan v2 v0.4 final - Word

Risk	Requirement
Non-compliance with data protection legislation regarding the exercise of data subjects' rights	• Risk assessment (fill in the DPIA)
Please justify your measure(s):	

Risk	Requirement
Disclosure of confidential information	• Indicate the methods used regarding the dissemination and publication of results, to avoid the disclosure of confidential information of partners • If applicable, store copies of personnel security clearances • State that partners complied with non-disclosure agreements and internal contracts in relation to research data
Please justify your measure(s):	

7. Data Protection Impact Assessment (DPIA) for WP3 activities

7.1. General

Name of organisation:

Role: is your organisation **a data controller or a data processor**?
Data controller is defined as the entity which 'determines the purposes and means of the processing of personal data'.
Data processor 'processes personal data on behalf of the controller'.

Names of personnel involved in the process:

Will the Data Protection Officer's (DPO) counsel be sought? If yes, please identify the DPO:

Will there be opportunities for data subjects or their representatives to present their views?
If yes, please explain:

7.2. Personal data

7.2.1. Collection of personal data

	YES	NO
Does your COMPACT activity require you to collect any personal data?		

If yes, please continue.

Describe the types/categories of personal data that will be collected (e.g. age, gender, level of education, etc.):

Explain the purpose(s) of data collection:

Explain the process of data collection (when, how, information sheets, informed consent forms, other documents, etc.):

Please fill in the following:

	YES	NO
Will the data be combined with other data from outside the program/change?		
Can the collected data become personal data due to links to third parties?		
Will the activity require you to collect personal data from other systems?		
Does your organisation collect only as much data as is necessary for the specific purpose(s) of data processing?		
Will data be stored for a limited period of time?		
Are you aware of the impact on data subjects' privacy?		
Are data subjects informed of their rights?		
Are data subjects able to control which data are collected?		
Are they able to control (i.e. rectify, erase, object to processing) their data after it has been collected?		
Can data subject ask for a declaration as to whether their data is being processed (right to access)?		
Can data subjects receive data concerning themselves, which has been or is being processed (right to data portability)?		

7.2.2. Re-use of personal data

If your activity does not require you to collect any new personal data, please fill in the following:

	YES	NO
Does the activity require you to use previously collected personal data?		

If yes, please answer the following questions.

Please identify the owner of the dataset(s) (name, other important information):

Please identify the type of personal data previously collected:

Please fill in the following:

	YES	NO
Is data openly and publicly available (open source)?		
Do you have permission from the owner to use these dataset(s)?		
Do you possess informed consent forms, information sheets and other relevant documents from the previous collection?		

7.3. Data processing

What is the nature, scope, context, and purpose of the processing?

Is recording of personal data, recipients and period for which the personal data will be stored ensured?

How does the processing operation function?

How and where is personal data stored (hardware, software, networks, people, paper etc.)?

Does the processing comply with any approved code of conduct in the sense of Art. 40 of the GDPR?[11]

[11] See Article 40 of the GDPR – such codes of conduct must be approved by the competent Data Protection Authority.

www.compact-project.eu
Funded by Horizon 2020
2017-19

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

HALL health & ageing law lab

TeNDER

Pseudonymising or encrypting data

- **Pseudonymisation**: "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject **without the use of additional information**, provided that such additional information is **kept separately** and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person"

=/= anonymisation!!

- Data masking: cannot identify without additional piece of info
- This other info is kept separately
- **Pseud data = still personal data!**

Records of processing activities

- Art. 30

- Keep logs of any processing of personal data (including access, consultation etc. internal to the org.)

- Logs to contain info:
  - WHO (name of the org.)
  - WHY processing
  - ABOUT WHOM (data subjects)
  - WHICH personal data
  - TO WHOM the data have been disclosed (internal/external)

Research without PD

- Synthetic data

= ML generated data

  - Research on covid-19 – 2021 paper
  - Use in clinical trials – 2021 paper
    - "To create synthetic data, a machine learning generative model is constructed from the real individual-level data, capturing its patterns and statistical properties. Then new data are generated from that model."
  - FAIR data sharing
  - Tutorials – Replica Analytics

- Helps avoid the "extra consent" problem + no need to apply the GDPR rules to the synthetic dataset!

Other additional measures

- Not an exhaustive list!
- Consider using additional informed consent, physical & digital security measures (e.g. accessibility of servers), choose local hosting instead of cloud-based …
- Check if university policy exists and what are the relevant procedures

GDPR: recap

1. Who is covered by the GDPR?
   - Controller & processor who process personal data
2. Personal data
   - Any piece of information relating to an individual
   - Wide definition – as long as the individual can be ID'd
   - Sensitive personal data – health, sexual orientation, political & religious beliefs…
3. Data quality principles
   - Personal data shall be…
   - Keep an eye on: which data, where, why and how
4. Specific rules for research – reuse of data
5. Safeguards
   - E.g. DPIA, pseudonymisation, synthetic data…

Commission's research ethics rules

For Commission-funded projects (incl. MSCA, H2020, ERC…)

VUB LSTS LAW, SCIENCE, TECHNOLOGY & SOCIETY RESEARCH GROUP

HALL health & ageing law lab

TeNDER

General guidelines on ethics

- Rules applicable to **all EU funded grants** https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-complete-your-ethics-self-assessment_en.pdf
- Does your proposal raise issues in any of the following categories? → add an ethical self-assessment to the application

1. Human embryonic stem cells (hESCs) and human embryos (hEs) *(HE, and EDF)*
2. Humans *(all EU Programmes)*
3. Human cells or tissues *(all EU Programmes)*
4. Personal data *(all EU Programmes)*
5. Animals *(all EU Programmes)*
6. Non-EU countries *(all EU Programmes)*
7. Environment, health and safety *(all EU Programmes)*
8. Artificial intelligence *(all EU Programmes)*
9. Other ethics issues *(all EU Programmes)*
10. Crosscutting issue: potential misuse of results *(all EU Programmes)*

General guidelines on ethics

- Questionnaires
  - Yes/no
  - Provide information and documents
    - At the time of application
    - During the research phase

- E.g. – involvement of human participants (Section 2)
  - As part of the proposal: 1) Details on recruitment, inclusion and exclusion criteria and informed consent procedures. 2) Details on unexpected findings policy
  - During research: 1) Copies of ethics approvals (if required by law or practice).
    2) Informed consent forms and information sheets.

Specific guidelines on other subjects

- Ethics & data protection: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-and-data-protection_he_en.pdf
  - Decision tree tool: https://ec.europa.eu/assets/rtd/ethics-data-protection-decision-tree/index.html
- Social sciences & humanities: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-in-social-science-and-humanities_he_en.pdf
- Research in developing countries: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/global-code-of-conduct-for-research-in-resource-poor-settings_he_en.pdf

Etc.

- Check the general guidelines + specific area of concern
- The guidelines apply together with the law!

Other rules?

European Health Data Space

- Proposal for EU HDS
  - Only for **health data** (e.g. clinical studies, psychology, wellbeing, working with patients, disabled populations, HIV positive participants …)
    - Personal and non-personal health data (e.g. population level, lab reports…)
  - Currently debated at EU level what the rules should be

https://www.politico.eu/article/5-things-to-know-about-the-eus-health-data-space/

https://www.law.kuleuven.be/citip/blog/a-close-look-at-european-data-spaces-and-usage-control/

Other rules?

Data Governance Act

- Proposal for the DGA
  - i) enhancing the availability of public sector data, the use of which is subject to third party rights (e.g., personal data, copyright, confidential information or trade secrets);
  - ii) regulating data intermediation services (data sharing services (DSS));
  - iii) establishing "data altruism" organisations addressing the need for a structure where data holders could share their data for purposes serving to the common good of the society.

- Altruistic data sharing = data holders sharing their personal or non-personal data for the purposes of general interest (e.g., scientific research purposes or improving public services) without seeking a reward
  - Likely involving research institutions such as universities, university hospitals…

https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/

The practical stuff

Putting the DP into a DMP

- When/how to address data protection/privacy in a DMP?
- Unless specifically stated (e.g. in the application), generally two options:
  - Address DP & DMP in the same document
    - Project COMPACT (H2020, 2017-19)
  - Address separately
    - TeNDER (H2020, 2019-2023)
    - The legal report is available [on the website]

} Sample provided!

The practical stuff

DPIA & gathering informed consent

We are building an app that elderly patients, living in care homes, can use to monitor their symptoms on a daily basis. The data resulting from the monitoring can also be accessed by their doctor, nurse and selected family member.

<u>How would you address possible risks to the patient's privacy?</u>

(feel free to be creative and make things up!)

To test the app, we want to recruit some patients from the nearby care home, since their feedback will be important for the developers.

<u>What kind of information should the consent form contain?</u>

Food for thought – how to convey this info to a person experiencing cognitive decline (Parkinson's, Alzheimer's, other forms of dementia…) in a way they can understand?

How would you answer those questions regarding your own PhD project?

Thank you!

danaja.fabcic.povse@vub.be

danajafp

https://lsts.research.vub.be/

https://hall.research.vub.be/

http://www.tender-health.eu/