Déléguée à la protection des données

The fundamentals of the protection of personal data

PhD student training 2022

Héloïse Faivre, Shared DPO

Grenoble-Alpes University, Savoie- Mont Blanc University, Grenoble INP (Polytechnic Institute) and Grenoble Sciences Po (French Institute of Political Sciences)

Definitions

Definition of "personal data”

- GDPR (Art. 4.1) ‘***“personal data” means any information relating to an identified or directly or indirectly identifiable natural person*** *[…], in particular through reference to an identifier such as a name, an identification number, location data or an online identifier, or to one or more precise elements specific to his/her physical, physiological, genetic, psychological, economic, cultural or social identity’*

Sensitive personal data

- Sensitive data (Art. 9 GDPR – Art. 6 Loi I&L (French Freedom of Info Act))
  - *'personal data that may reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person,* ***data concerning the health*** *or data concerning the sex life or sexual orientation of natural persons'*

Processing for research purposes is possible, but requires the completion of a Privacy Impact Assessment with the DPO

Health data

- Health data: from and until when?
  - The concept of health data is **broadly defined by the GDPR**
    - (GDPR Consid. 35) *Personal data concerning* ***health should include any data pertaining to the health status of the person concerned that reveals information relating to the past, present or future physical or mental state of health of the person concerned****. […*
    - (GDPR Art. 4.15) *"data concerning health", personal data relating to the physical or mental health of a natural person – including the provision of healthcare services – that reveals information about such a person's state of health*;
  - Gathering data: various procedures
    - <u>direct collection</u> from the individual (oral, questionnaire, etc.)
    - a person's <u>measurements</u>: EEG, ECG, respiratory volume, etc.
    - <u>inference</u>: possibility of deducing new information about an individual (calculations, data-matching, etc.)

e.g. height + weight →BMI = health data

→ to be assessed on a case-by-case basis, taking into account the nature of the data gathered and processed → <u>with the DPO</u>

Other definitions

- **Processing**: any operation(s) carried out on personal data, whether automated or not, from its collection to its deletion
- **Individual concerned**: the natural person to whom the collected and processed data relates
  - **e.g.**. participant(s) in research (and investigators) ; laboratory members, etc.
- **Recipient(s)**: any individual or group of individuals or body to whom personal data is communicated
  - **e.g. administrative processing** → trustees, HCERES (High Council for the Evaluation of Research and Higher Education), etc.
  - **e.g.**. **research processing** → making research data available
- **Pseudonymisation**: measures applied to personal data so that a natural **person cannot be identifiable by his/her data without recourse to additional information** […] stored **separately** and subject to measures preventing the identification of such a person
  - e.g. in research: lookup table: [volunteer's identity / anonymous number]
    research data: [anonymous number + non-identifying personal data]

The main applicable laws

- the **General Data Protection Regulation (GDPR)**
  - THE EUROPEAN PARLIAMENT AND COUNCIL’S (EU) REGULATION 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free circulation of such data
  - **uniformly applied within the EU since 25 May 2018**

- the **Loi Informatique et Libertés (French Freedom of Information Act)** [**GDPR + HEALTH AND POLICE/JUSTICE SECTORS**]
  - Amended Law no. 78-17 of 6 January 1978 on data processing, files and freedoms

What does the Law say?

5 Basic Principles to be observed

1. the **purposes** of the processing: objectives behind the (direct or indirect) gathering of personal data

→ lawful, specific, explicit and legitimate

2. the **minimisation** and **relevance** of the data

→ required for the purposes and not excessive

3. **limited data storage period**

→ limited to the period strictly necessary for the purposes

4. **data security** (continuity and integrity) **and confidentiality**

→ proportionate to the purposes and the data being processed

5. **respecting people's rights** :

→ **information**, access, objection, deletion, withdrawal, etc.

Lawfulness (Art. 6 of the GDPR) ‘Do I have the right to process this data?’

→ **at least one of the 6 legal bases**

1. **individuals’ free and informed consent**

   →after providing individuals with statutory information that is appropriate, comprehensive, clear and concise

   →common practice within research involving individuals

2. execution of a **contract** to which the individual concerned is party
3. **legal obligation** to which data controllers are subject
4. **vital interest** of natural persons (individual concerned or another natural person)
5. **carrying out a public interest mission**

   → legal basis for research processing

6. **legitimate interest** on the part of a data controller

The GDPR principles to be observed when processing data

- **liability and proof of compliance**

data controllers must be able to prove their compliance at all times

  - → laboratory processing record + processing documentation (e.g. CERGA (Grenoble-Alpes Research Ethics Committee) files)

- **minimisation of gathered data**

- **end-to-end data protection for projects** (*privacy by design*)

The GDPR principles to be observed when processing data

Déléguée à la protection des données

- **data protection by default** (*privacy by default*): everyday organisation, practices and tools
  - → **securing researchers'** computers (recommended tool: VeraCrypt)
  - → **encrypt** recordings, photos (group photos), confidential and sensitive data, etc.
  - **do not attach files containing personal data to emails**
    - → **use a secure filing/downloading service** (e.g. RENATER's FileSender)
- **Data Protection Impact Assessment** (DPIA)
  - for processing that may pose a high risk to the rights and freedoms of natural persons

Some areas requiring vigilance

- **image rights and voice rights**
  - **The collection, storage and use of photos (group photos) and video and audio recordings are subject to the individuals' express consent (authorisation)**
- **minimisation of gathered data**
  - → e.g. gather an age group or age but not a date of birth
  - → e.g. use closed lists (inclusion, etc.) → question: 'does at least one item concern you?'
- **beware of implicit data (risk of identification through matching with other research data)**
  - **e.g.1**. study of children attending ***the xxxxx preschool in Grenoble*** *+ collection of***parents' professions**

Some areas requiring vigilance

- Anonymisation vs pseudonymisation
  - Anonymisation→ direct or indirect identification **impossible**
  - pseudonymisation → identification impossible **without additional information**
- Digital tools: Beware of free “mainstream” platforms!
  - Use internal tools or infrastructures instead ((GRICAD, MSH, etc.)
  - Prioritise tools that are subject to European law

In research

link between ethics and personal data protection

Ethics resources

- *Fédération des Comités d'éthique pour les recherches (French Federation of Institutional Research Ethics Committees, FCER)*
- *Comité d'éthique pour la recherche (Research Ethics Committee), Grenoble-Alpes (CERGA) [Carole Peyrin]*

2 distinct <u>but strongly linked areas</u>

Ethics in research (on and with natural persons)

- Respect for the universal principles of human dignity and the primacy of the human being
  - Public interest
  - Philanthropic purposes and approach: “benefit/risk balance”
  - Participants’ autonomy and free will
  - free and informed consent
  - Justice, equity and impartiality
  - Rigour and scientific integrity
- Statutory or binding frameworks
  - Nuremberg Code (1946)
  - Helsinki Declaration (1964)
  - Health: Law of 5 March 2012 on research involving the human person (“Jardé Act”) French Public Health Code

Protecting personal data in research

- Respecting the rights and freedoms and privacy of natural persons
  - Lawfulness (public interest)
  - Legitimacy and proportionality
  - loyalty
  - Information, consent or objection, limitation, etc.
  - Legal compliance
- Statutory frameworks
  - GDPR (2016)
  - Freedom of Information Act (1978)
  - Health: Law of 5 March 2012 on research involving the human person (“Jardé Act”) French Public Health Code

Further resources

the CNIL’s (very extensive!) website
www.cnil.fr

General Data Protection Regulation
https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

Freedom of Information Act
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460

Ethics and GDPR research (Fédération des CER et SupDPO, Federation of CERs, and the Network of Higher Education, Research and Innovation DPOs)
https://pod.univ-lille.fr/ethique-et-protection-des-donnees-en-recherche/

Ethics (CERGA)
http://www.grenoblecognition.fr/index.php/ethique/ (RUBRIQUE ÉTHIQUE)

Thank you for your time