GDPR - myths and reality

Short introduction for researchers

(based on slides from) Dr Monica Cappelletti

(formerly) Post-doc, School of Law&Gov, DCU

ASGARD and VOX-Pol projects

Structure

- Data Protection v. Privacy
- Personal Data and types of Data
- Data Protection Principles
- Data Protection Principles for designing tools
- Legal challenges and risks
- Case-studies in research domain

GDPR?

- General Data Protection Regulation
- European Union-wide framework came into effect on 25 May 2018
- Purpose: protect mis-use of sensitive and personal data

GDPR?

- Data Controller: organisation or company that decides the methods to use for personal data
- Data Processor: performs the processing on behalf of the Controller
- Data Protection Officer (DPO): formal role in organisation
- Data Subject: person whose data it is
- Data Breach: “A data breach is any unauthorised, unlawful or accidental disclosure, destruction, loss, alteration or access to personal data.”
- What should you do? Inform the DPO

https://www.dcu.ie/sites/default/files/info/3bidb_proc-public-final.pdf

But why GDPR and research?

Data Protection v. Privacy Rights

Data Protection

Article 8 (Protection of Personal Data) of the EU Charter of Fundamental Rights:

"*1. Everyone has the right to the protection of personal data concerning him or her.*

*2. Such data must be processed **fairly** for **specified purposes** and on the basis of the **consent of the person** concerned or some other **legitimate basis** laid down by law. Everyone has the **right of access** to data which has been collected concerning him or her, and the **right to have it rectified**.*

3. Compliance with these rules shall be subject to control by an independent authority."

Privacy

Article 7 (Respect for private and family life) of the EU Charter of Fundamental Rights:

"Everyone has the right to respect for his or her private and family life, home and communications."

Personal Data

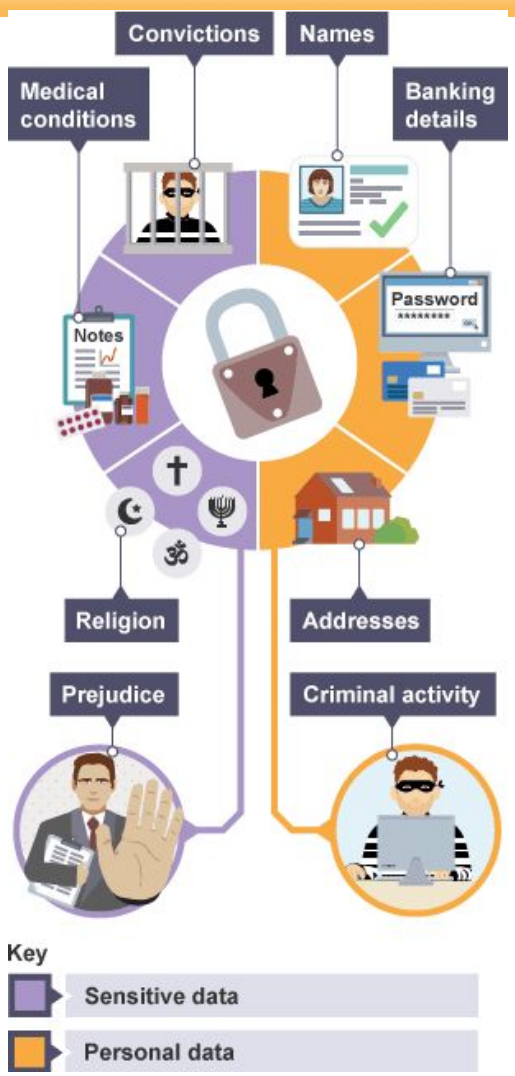
Any **information** relating to an **identified or identifiable** natural **person** ("data subject");

an identifiable person is one who **can be identified, directly or indirectly**, in particular by reference to an identification number, location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data may be **processed** only if the data subject has **unambiguously** given his/her **consent** ("prior consent").

(art. 4, n. 1), Regulation (EU) 2016/679)

Different types of Personal Data



Sensitive (Personal) Data (Special categories)

Personal data revealing **racial** or **ethnic origin, political opinions, religious or philosophical beliefs**, **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**.

Sensitive data may be processed only if the data subject has given his/her **explicit consent** to the processing of those data ("prior written consent").

(art. 9, Regulation (EU) 2016/679 + art. 10)

Different types of Personal Data

Genetic Data:

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, n. 13), Regulation (EU) 2016/679)

Biometric Data:

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, n. 14), Regulation (EU) 2016/679)

Data Processing and Profiling

Processing

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.**

(Art. 4, n. 2), Regulation (EU) 2016/679)

Profiling

Any form of **automated processing** of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to **analyse** or **predict** aspects concerning that natural person's performance at **work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements**.

(Art. 4, n. 4), Regulation (EU) 2016/679)

Different types of Data and Process

Anonymisation

Processing of data with the aim of removal of information that could lead to an individual being identified. Data can be considered anonymised when it does not allow identification of the individuals to whom it relates, and it is not possible that any individual could be identified from the data by any further processing of that data or by processing it together with other information which is available or likely to be available. Use of anonymised data does not require the consent of the “data subject.”

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.

(Art. 4, n. 5), Regulation (EU) 2016/679)

Do not forget: ENCRYPTION

Tell me about Will …

https://public.tableau.com/en-us/gallery/tell-me-about-will
https://www.abc.net.au/news/2015-08-16/metadata-retention-privacy-phone-will-ockenden/6694152
https://vimeo.com/136721058

Be cautious about “anonymized” data!

Different types of Data and Process

Open Data

Data that can be freely used, re-used, and redistributed by anyone – subject only, at most, to the requirement to attribute and share-alike [Open data Handbook]

Simulated Data

Imitation or creation of data that closely matches real-world data, but is not real world data. For these data, consent is not necessary since it is not possible to identify the “data subject.”

Personal Data: to sum-up

Personal Data	Open Data	Fake/ Simulated Data
Data about a person (REAL PERSON)	Data about people (not a person)	Data about people or an invented person (like a fiction)
Sensitive or not sensitive	Data of public domain	
Necessary to be collected, used and profiled: **CONSENT** of that person	**Free available**	**Free available**

Data Protection Principles I

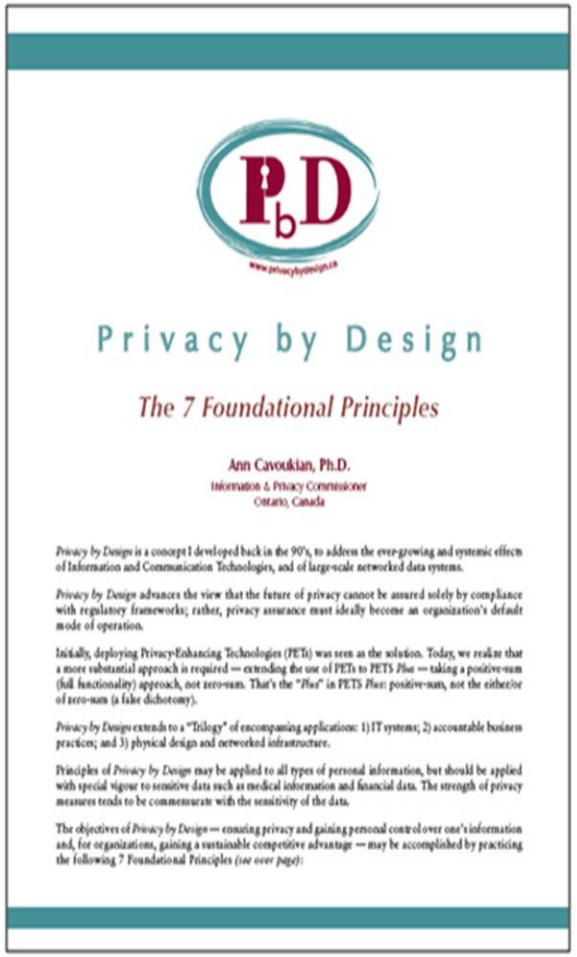
1. Personal data must be obtained and processed **fairly, lawfully, and *in a transparent way***
2. Personal data should only be collected for **specified, explicit, and legitimate purposes – PURPOSE LIMITATION**
3. Personal data should be used in an **adequate, relevant, and not excessive way** – **DATA MINIMISATION**
4. Keep personal data **accurate, complete, up-to-date - ACCURACY**
5. **Retain** personal data for **no longer** than is necessary - **STORAGE LIMITATION**
6. Keep personal data **safe and secure - INTEGRITY and CONFIDENTIALITY**
7. **Accountability**
8. **No transfer of personal data overseas**

(art. 5, Regulation (EU) 2016/679)

Privacy by Design:

The 7 Foundational Principles

1. ***Proactive*** not ***Reactive***:
   Preventative, not Remedial;
2. Privacy as the ***Default*** setting;
3. Privacy ***Embedded*** into Design;
4. ***Full*** Functionality:
   Positive-Sum, not Zero-Sum;
5. End-to-End **Security**:
   Full Lifecycle Protection;
6. Visibility **and** Transparency:
   Keep it **Open**;
7. Respect for User Privacy:
   Keep it **User-Centric**.



PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

PbD

www.privacybydesign.ca

Legal challenges and risks

- Data Protection (legal requirements + technical requirements + civil liabilities)
- Copyrights
- Criminal activities (incidental findings)
- Ethical

Case-study I in research domain

Hard disk/mobile disk copies

- Will you use/copy a computer/mobile that you have stumbled upon?
- It could have been stolen!
- LEGAL/DP ISSUE

WE CANNOT USE!

Case-study II in research domain

Boards.ie

- "Popular Irish bulletin board site, offering web hosting, chat rooms, and news group access"
- Open source, not protected password

Ashley Madison

- "Canadian online dating service and social networking service marketed to people who are married or in committed relationships" [Wiki]
- **Closed network, protected by password**

6 Key Points

1. Data = Person
2. Consent of person
3. Purpose = reason of collection data
4. Data security
5. Think of DP issues before starting
6. ‘Free’ on-line does not mean legal!

Consider …

1. What if you're talking with a colleague and think that your patient test data (health records) might help them in their cancer treatment research? Can you **let them use your data**?
2. Someone breaks into your lab and steals a laptop with sensitive personal data on it! **What do you do?**
3. If everyone has the **right of access** to their data, what do you need to record in your data or metadata?
4. But if you want to ensure that you are **not storing personal data**, what should you do in designing your data collection or storage?

Recent example

- Optus data breach in Australia in 2022
- ~10 million customers in total (unknown accessed)
- email addresses, home addresses and dates of birth
- ~2.8 million people also had their passport or license numbers
- Medicare numbers
- Even people who were no longer customers!
- No GDPR in Australia
- https://www.bridewellconsulting.com/how-the-gdpr-could-have-reduced-the-impact-of-the-optus-data-breach

Resources

- https://www.citizensinformation.ie/en/government_in_ireland/data_protection/overview_of_general_data_protection_regulation.html
- https://www.dataprotection.ie/
- https://www.dcu.ie/ocoo/data-protection.shtml
- https://www.dcu.ie/ocoo/dp/guides.shtml
- https://www.dcu.ie/sites/default/files/ocoo/docs/1_dp_help sheet_-_7_principles_-_v5.pdf