LLMs in the Cloud: Compliance and Data Protection

Fabian Prasser

Ethical and Legal Framework

Regulations and roles when using personal data

Privacy

- Privacy: “Someone's right to keep their personal matters and relationships secret” [1]
- Information privacy: Right to control personal information and how it is used, processed and collected

EU Charter of Fundamental Rights

Article 7: Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.

Data Protection

- “Data protection is about protecting any information relating to an identified or identifiable natural (living) person” [1]
- Originates from the right to privacy
- Among other things, privacy and data protection require information security

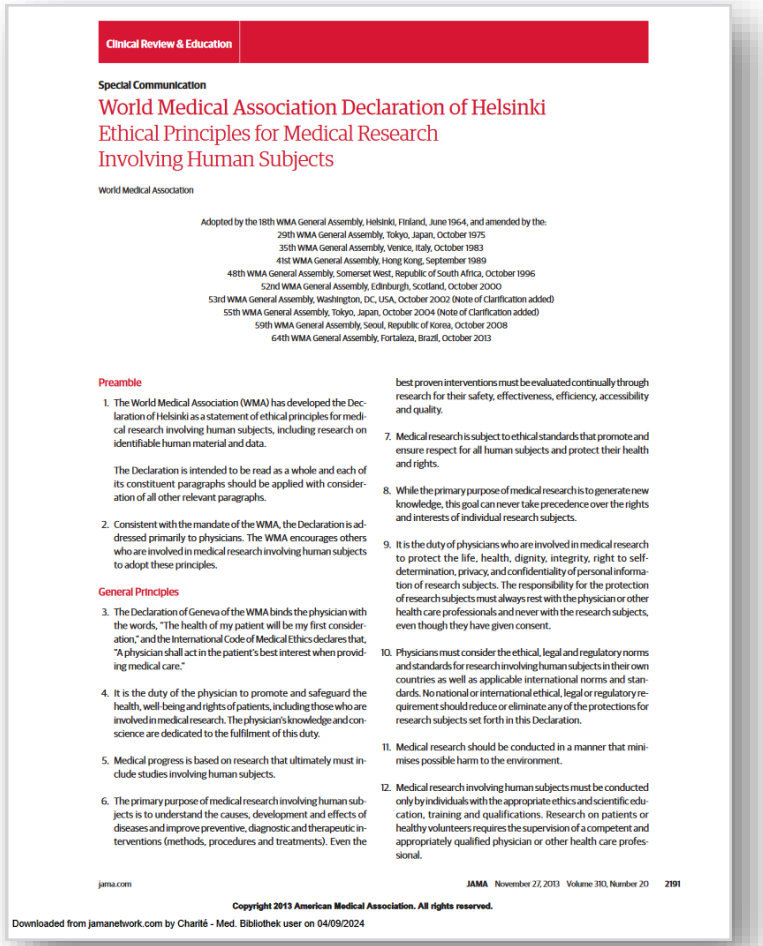
EU Charter of Fundamental Rights

Article 8: Protection of personal data

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.

Declaration of Helsinki

- **Guidance** for **research involving human subjects**, including identifiable human **material and data (1964)**
- **Proposed research:**
  - Has to has to have a **sound scientific basis**
  - Needs to be conducted by suitably **qualified individuals**
  - Has to be subject to **ethical oversight**
- Emphasizes the importance of an **informed consent:**
  - Participants must be **informed** about the research, aware of its potential **risks and benefits,** and participating **voluntarily**
- Includes the special protection of **vulnerable groups**
- Formulates **requirements for publication** of research findings



Clinical Review & Education

Special Communication

World Medical Association Declaration of Helsinki
Ethical Principles for Medical Research
Involving Human Subjects

World Medical Association

Adopted by the 18th WMA General Assembly, Helsinki, Finland, June 1964, and amended by the:
29th WMA General Assembly, Tokyo, Japan, October 1975
35th WMA General Assembly, Venice, Italy, October 1983
41st WMA General Assembly, Hong Kong, September 1989
48th WMA General Assembly, Somerset West, Republic of South Africa, October 1996
52nd WMA General Assembly, Edinburgh, Scotland, October 2000
53rd WMA General Assembly, Washington, DC, USA, October 2002 (Note of Clarification added)
55th WMA General Assembly, Tokyo, Japan, October 2004 (Note of Clarification added)
59th WMA General Assembly, Seoul, Republic of Korea, October 2008
64th WMA General Assembly, Fortaleza, Brazil, October 2013

Preamble

1. The World Medical Association (WMA) has developed the Declaration of Helsinki as a statement of ethical principles for medical research involving human subjects, including research on identifiable human material and data.

   The Declaration is intended to be read as a whole and each of its constituent paragraphs should be applied with consideration of all other relevant paragraphs.

2. Consistent with the mandate of the WMA, the Declaration is addressed primarily to physicians. The WMA encourages others who are involved in medical research involving human subjects to adopt these principles.

General Principles

3. The Declaration of Geneva of the WMA binds the physician with the words, "The health of my patient will be my first consideration," and the International Code of Medical Ethics declares that, "A physician shall act in the patient's best interest when providing medical care."

4. It is the duty of the physician to promote and safeguard the health, well-being and rights of patients, including those who are involved in medical research. The physician's knowledge and conscience are dedicated to the fulfilment of this duty.

5. Medical progress is based on research that ultimately must include studies involving human subjects.

6. The primary purpose of medical research involving human subjects is to understand the causes, development and effects of diseases and improve preventive, diagnostic and therapeutic interventions (methods, procedures and treatments). Even the best proven interventions must be evaluated continually through research for their safety, effectiveness, efficiency, accessibility and quality.

7. Medical research is subject to ethical standards that promote and ensure respect for all human subjects and protect their health and rights.

8. While the primary purpose of medical research is to generate new knowledge, this goal can never take precedence over the rights and interests of individual research subjects.

9. It is the duty of physicians who are involved in medical research to protect the life, health, dignity, integrity, right to self-determination, privacy, and confidentiality of personal information of research subjects. The responsibility for the protection of research subjects must always rest with the physician or other health care professionals and never with the research subjects, even though they have given consent.

10. Physicians must consider the ethical, legal and regulatory norms and standards for research involving human subjects in their own countries as well as applicable international norms and standards. No national or international ethical, legal or regulatory requirement should reduce or eliminate any of the protections for research subjects set forth in this Declaration.

11. Medical research should be conducted in a manner that minimises possible harm to the environment.

12. Medical research involving human subjects must be conducted only by individuals with the appropriate ethics and scientific education, training and qualifications. Research on patients or healthy volunteers requires the supervision of a competent and appropriately qualified physician or other health care professional.

General Data Protection Regulation (1)

EU law on data protection and privacy in the European Union and the European Economic Area, that came into effect in 2018

Primary objectives

- Protect individuals' privacy and personal data
- Harmonize data privacy laws across Europe
- Empower individuals over their personal data

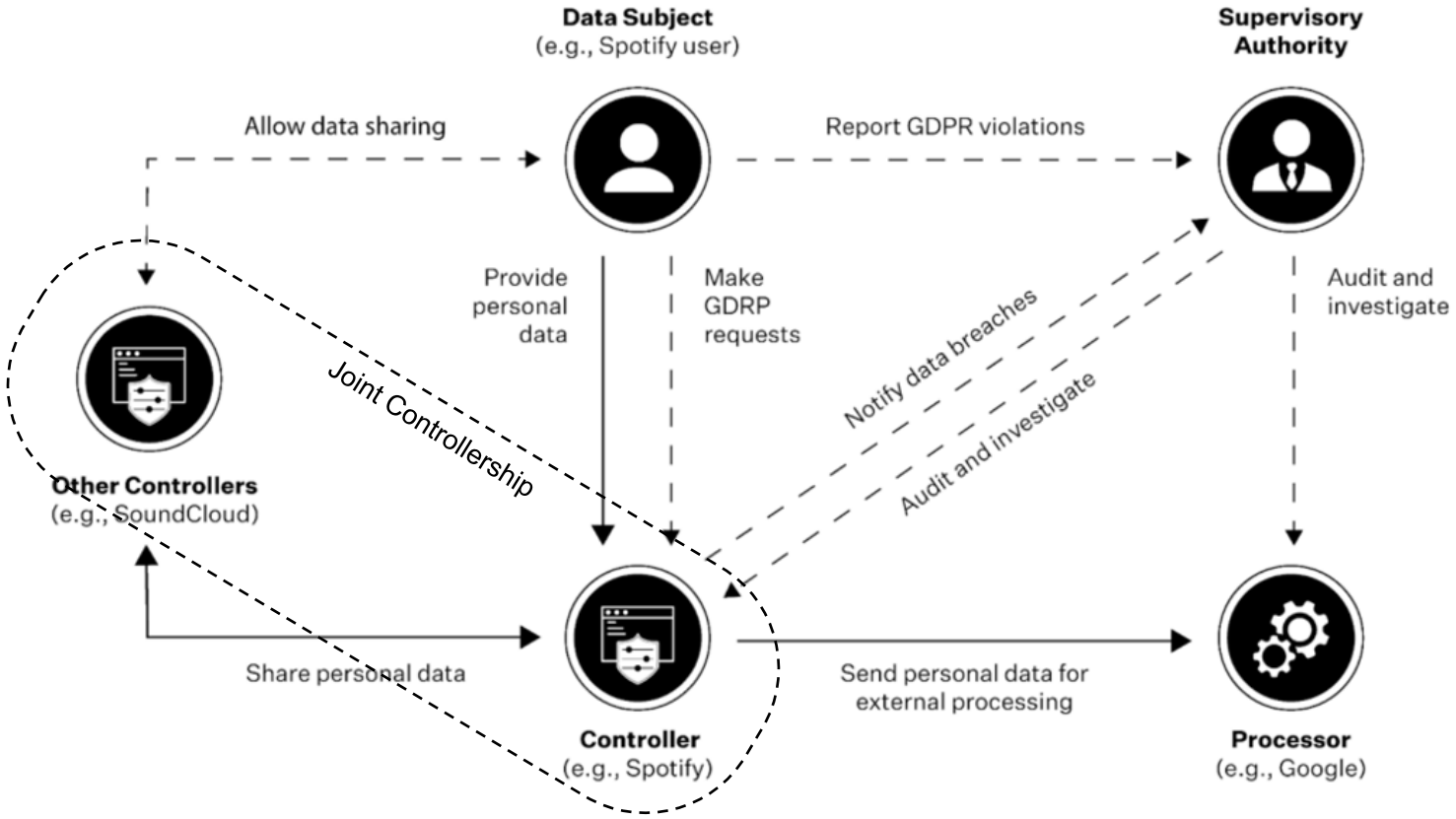
Principles: lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, integrity, and accountability

Rights of Individuals: right to access, rectification, erasure, and objection against data processing, rights to be informed about data breaches that could affect a person’s rights, right to not be subject of automated decision making

General Data Protection Regulation (2)

Roles: Subjects, controllers, processors

Legal basis: Processing is forbidden by default, can be allowed through consent or legal basis

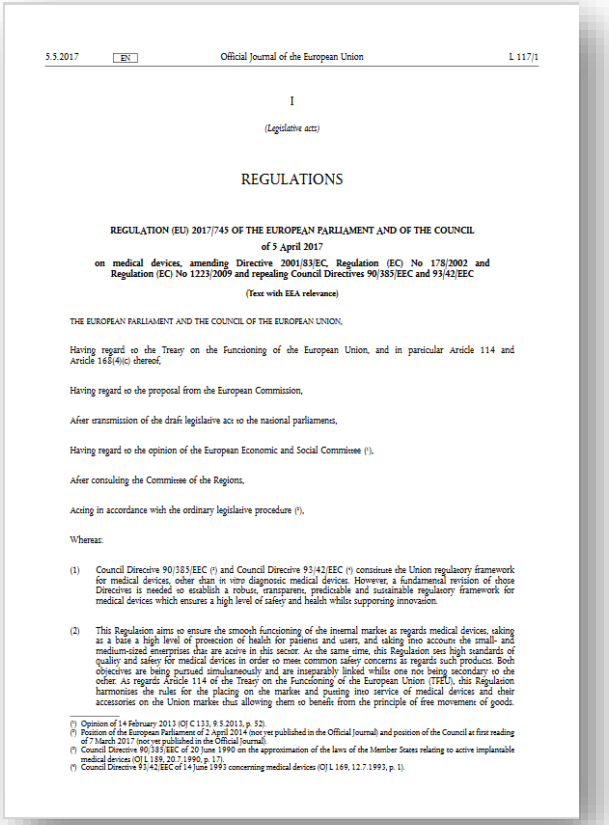


Data Protection vs. Information Security

- “Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **(A) integrity [..]; (B) confidentiality;** and **(C) availability** […].” (U.S. Code § 3542)
- “preservation of **confidentiality, integrity** and **availability** of information; in addition, other properties such as **authenticity, accountability, non-repudiation** and **reliability** can also be involved” (ISO/IEC 27000)
- Usually, information security refers to protecting the confidentiality, integrity, and availability of **systems** and **information against malicious or unintentional threats**

Medical Device Regulation (MDR)

- Covers all medical devices and their accessories **intended for diagnosis, prevention, monitoring, prediction, prognosis or treatment** of disease
- Classifies devices **based on the potential risk level** into
  - Class I (low risk): e.g. bandages, examination gloves
  - Class IIa (medium risk): e.g. surgical clamp
  - Class IIb (medium to high risk): e.g. contact lens solution
  - Class III (high risk): e.g. implantable pacemakers
- Software can also be a medical device, e.g.:
  - Image processing for diagnostic purposes
  - Clinical decision support systems
  - Software for controlling active implantable devices



5.5.2017 EN Official Journal of the European Union L 117/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 5 April 2017
on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

(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 114 and Article 168(4)(c) 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),

After consulting the Committee of the Regions,

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1) Council Directive 90/385/EEC (3) and Council Directive 93/42/EEC (4) constitute the Union regulatory framework for medical devices, other than in vitro diagnostic medical devices. However, a fundamental revision of those Directives is needed to establish a robust, transparent, predictable and sustainable regulatory framework for medical devices which ensures a high level of safety and health while supporting innovation.

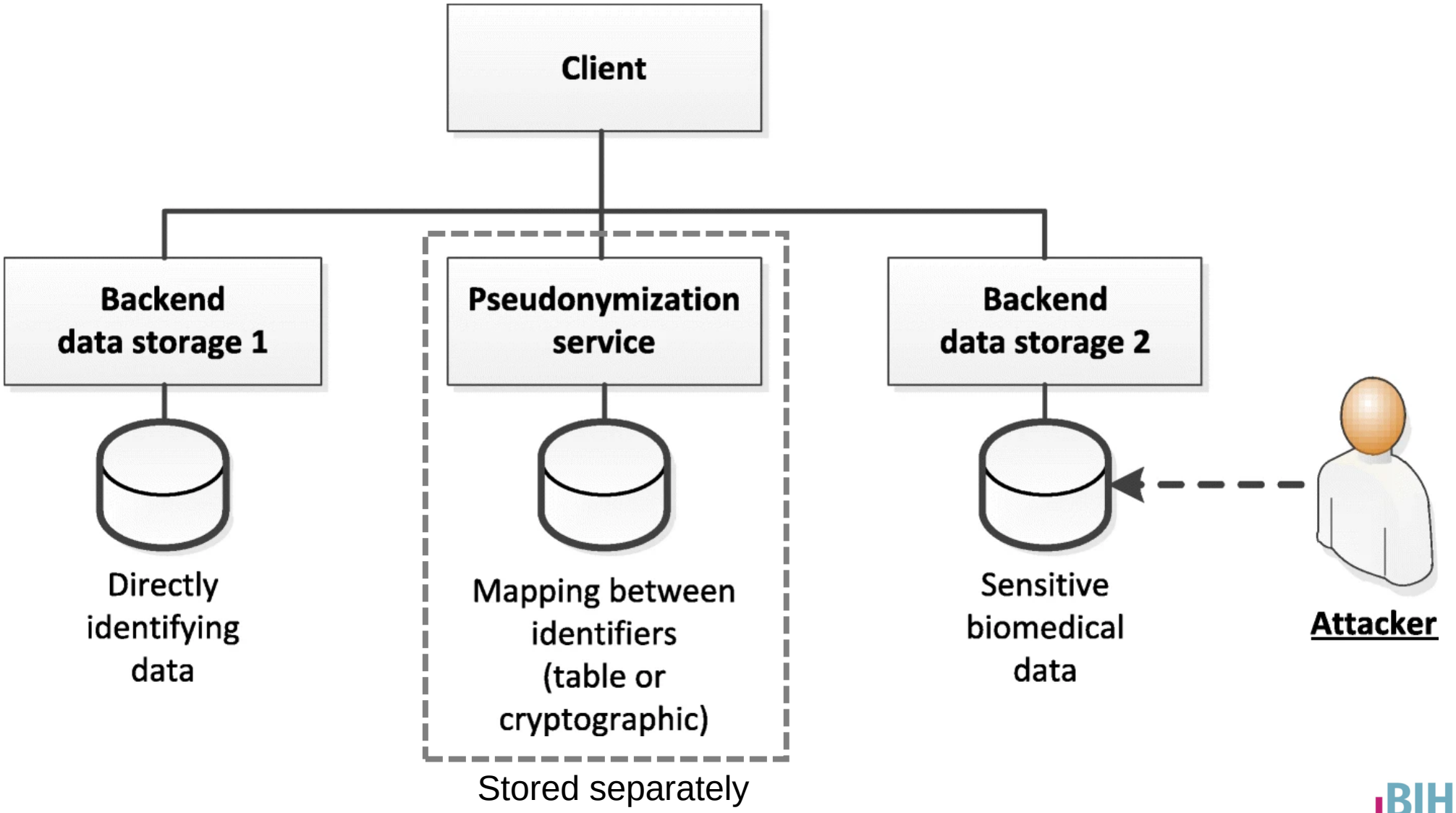
(2) This Regulation aims to ensure the smooth functioning of the internal market as regards medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small- and medium-sized enterprises that are active in this sector. As the same time, this Regulation sets high standards of quality and safety for medical devices in order to meet common safety concerns as regards such products. Both objectives are being pursued simultaneously and are inseparably linked whilst one not being secondary to the other. As regards Article 114 of the Treaty on the Functioning of the European Union (TFEU), this Regulation harmonises the rules for the placing on the market and putting into service of medical devices and their accessories on the Union market thus allowing them to benefit from the principle of free movement of goods.

(1) Opinion of 14 February 2013 (OJ C 133, 9.5.2013, p. 52).
(2) Position of the European Parliament of 2 April 2014 (not yet published in the Official Journal) and position of the Council at first reading of 7 March 2017 (not yet published in the Official Journal).
(3) Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices (OJ L 189, 20.7.1990, p. 17).
(4) Council Directive 93/42/EEC of 14 June 1993 concerning medical devices (OJ L 169, 12.7.1993, p. 1).

Basic Data Protection Methods

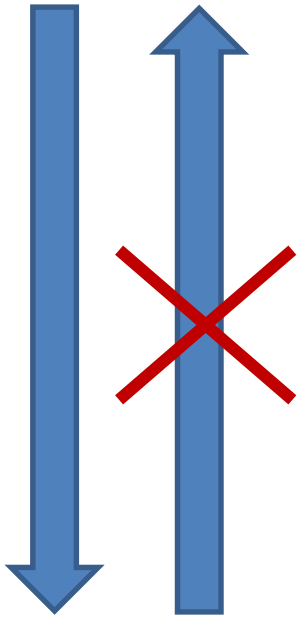
Measures to implement when training or using LLMs with personal data

Pseudonymization



Anonymization (1)

Personal data



Anonymous data

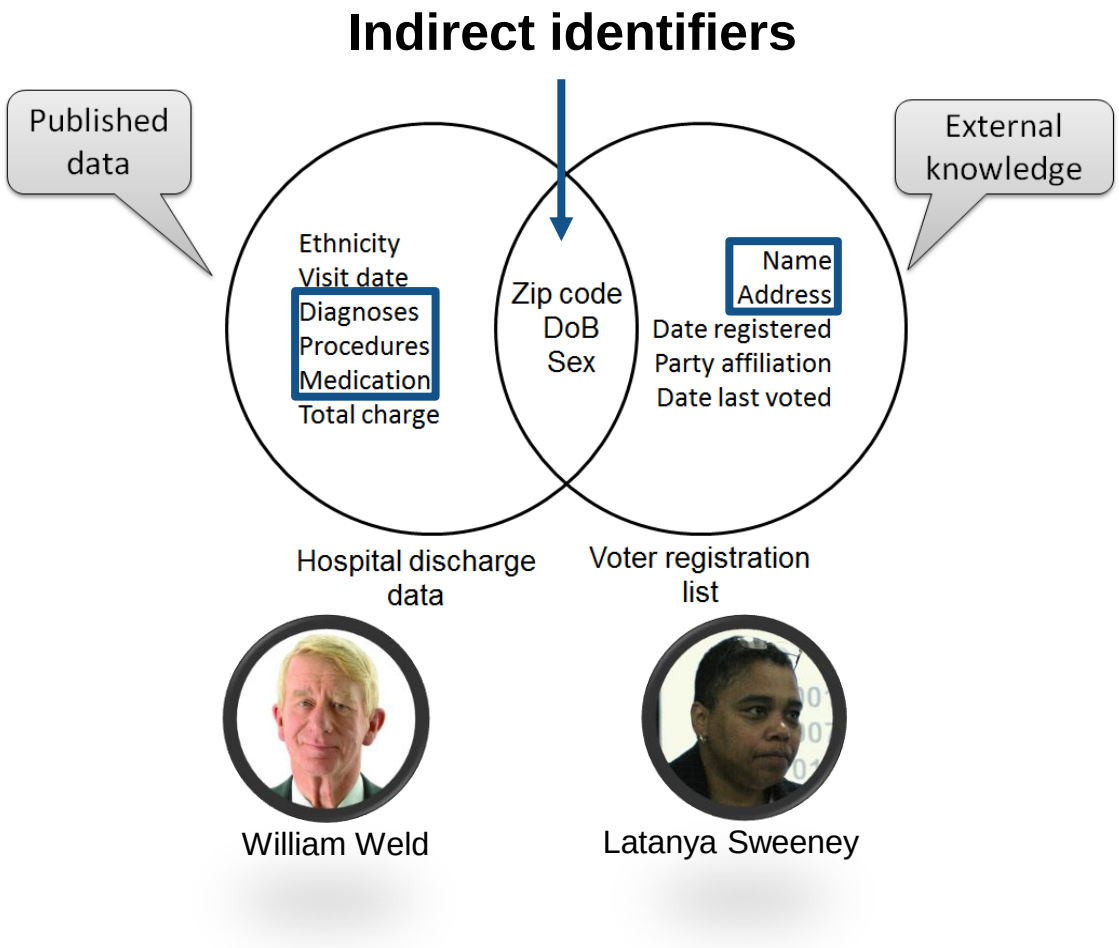
GDPR, Recital 26:

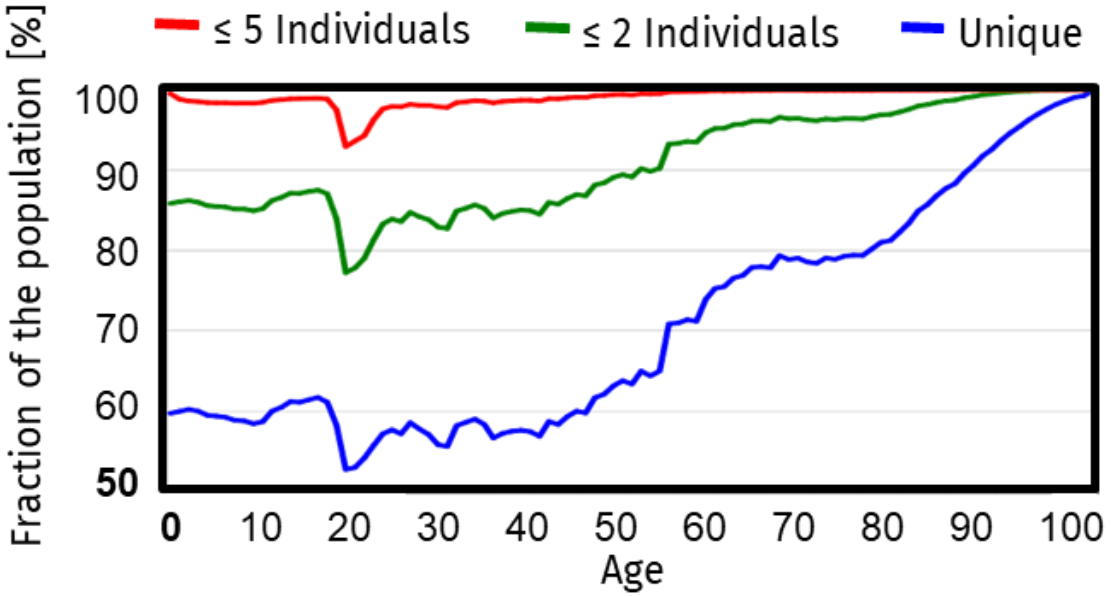
„The principles of data protection should **apply to any information concerning an identified or identifiable natural person** […]“

„[...] To determine whether a natural person is identifiable, **account should be taken of all the means reasonably likely to be used**, [..]to identify the natural person directly or indirectly [...]“

"[In doing so] all **objective factors, such as the costs of and the amount of time required** for identification, taking into consideration the **available technology at the time of the processing and technological developments** […]“

Anonymization (2)





~ 87% of the U.S. population can be uniquely identified by a combination of postcode, date of birth and gender

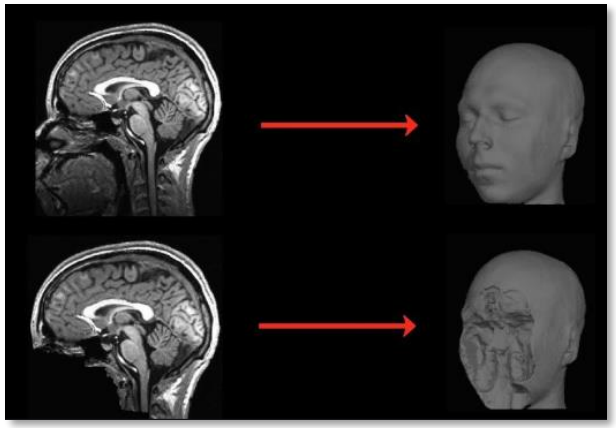
Sources: Golle P. Revisiting the uniqueness of simple demographics in the US population. 5th ACM Workshop on Privacy in the Electronic Society, 2006;
Sweeney L. Simple Demographics Often Identify People Uniquely. Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000;
Image Source: By Gary Johnson from Taos, NM - BillWeld5x7 (2), CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=49683363

Anonymization (3)

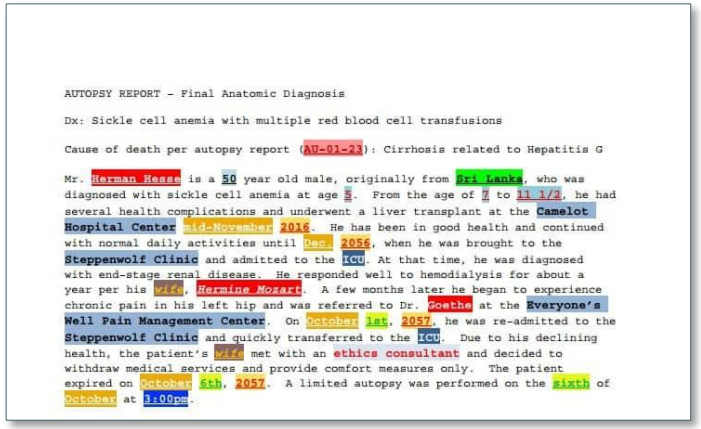
- **Demographic data** (Sweeney 1997; Golle 2006; El Emam 2008)
- **Diagnosis codes** (Loukides et al. 2010)
- **DNA (SNPs)** (Lin, Owen, & Altman 2004; Homer et al. 2008, Wang et al. 2009)
- **Pedigree structure** (Malin 2006)
- **Location visits** (Malin & Sweeney 2004, Golle & Partridge 2009)
- **Movie reviews** (Narayanan & Shmatikov 2008)
- **Search queries** (Barbaro & Zeller 2006)
- **Social network structure** (Backstrom et al. 2007, Narayanan & Shmatikov 2009)

⚠ **But: Unique ≠ Identified ≠ identifiable!**

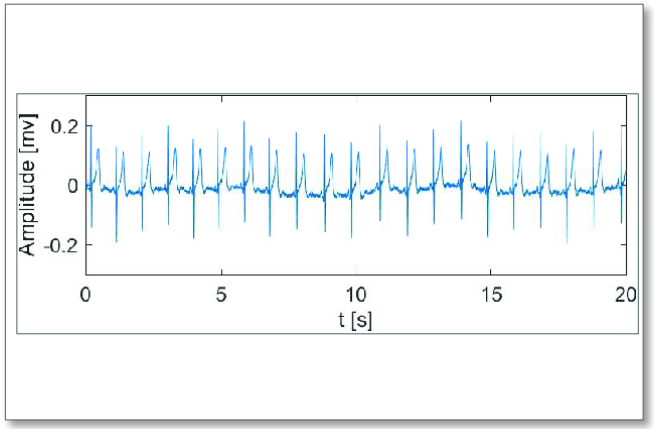
Anonymization (4)



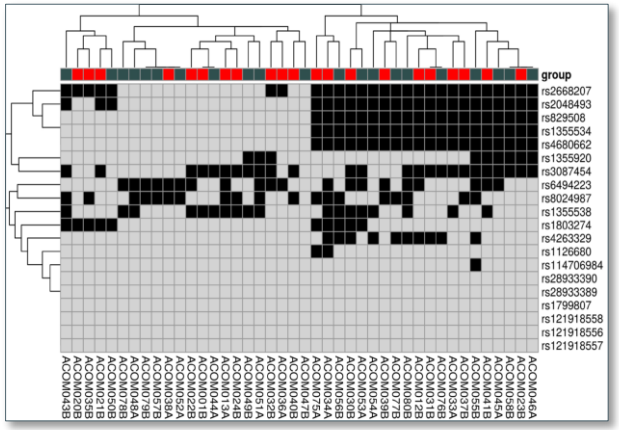
Source:
https://surfer.nmr.mgh.harvard.edu/fswiki/mri_deface



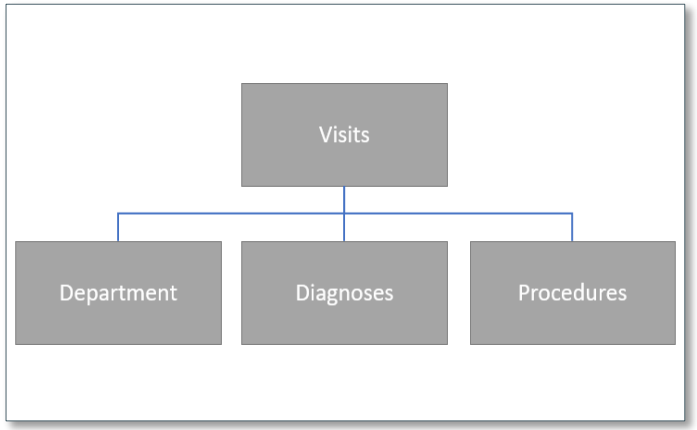
Source: https://scrubber.nlm.nih.gov/



Source: https://doi.org/10.1109/MeMeA.2018.8438751



Source: https://doi.org/10.2147/CCID.S176842



Source: https://www.g-drg.de/Datenlieferung_gem._21_KHEntgG

Onset of exposure	Yes	No	Total
20+ years***	339	53	392
0–19 years***	203	522	725
Total	542	575	1,117

Source: https://doi.org/10.1080/10937404.2012.678766

Minimization

Purpose Limitation

- Data should only be collected and processed for clearly defined, legitimate, and specific purposes

Data Limitation

- Collect and process only the minimum amount of data necessary to achieve the intended purpose

Retention Control

- Retain personal data only for as long as it is necessary to fulfill the purpose

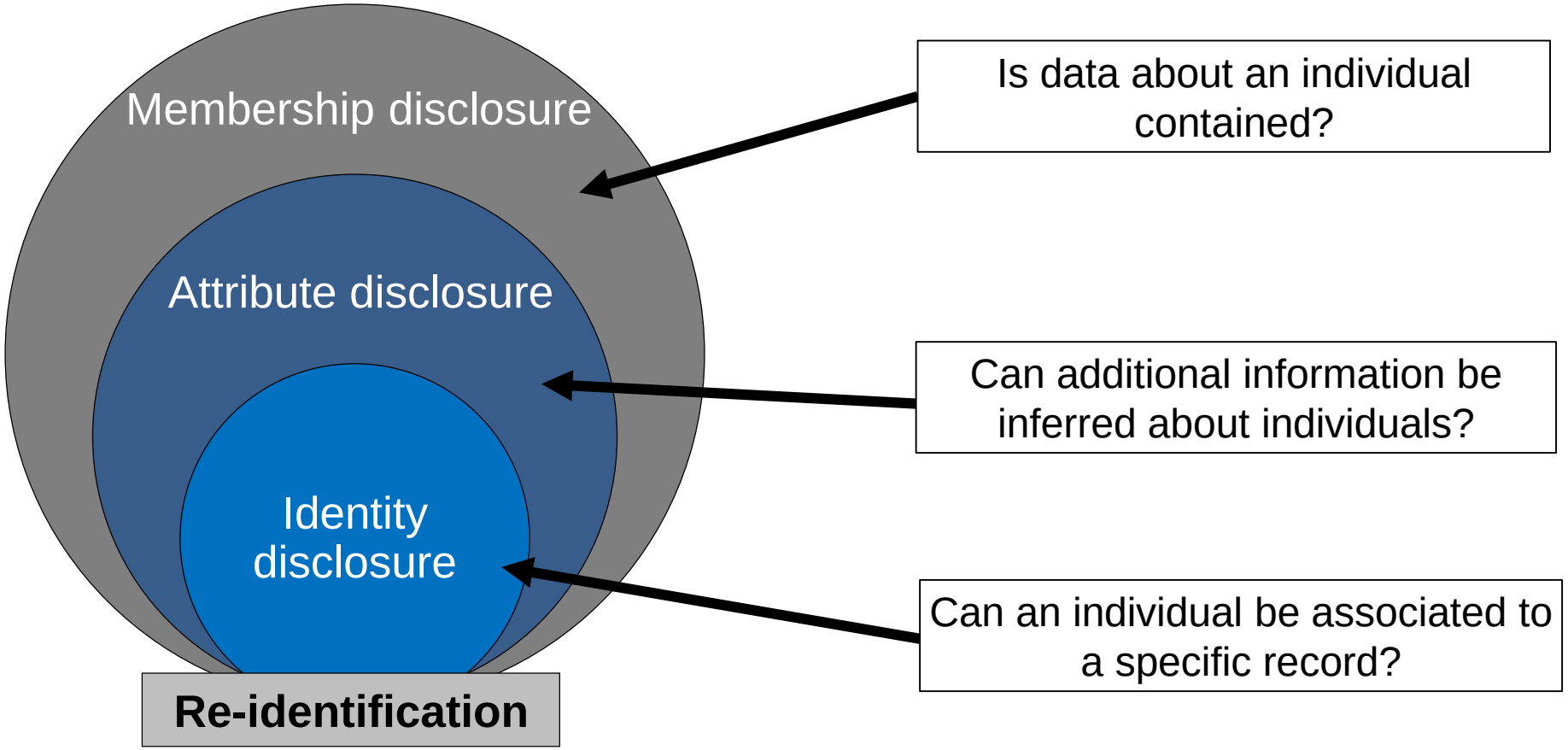
Advanced Data Protection Aspects

Aspects to consider when training or fine-tuning LLMs using personal data

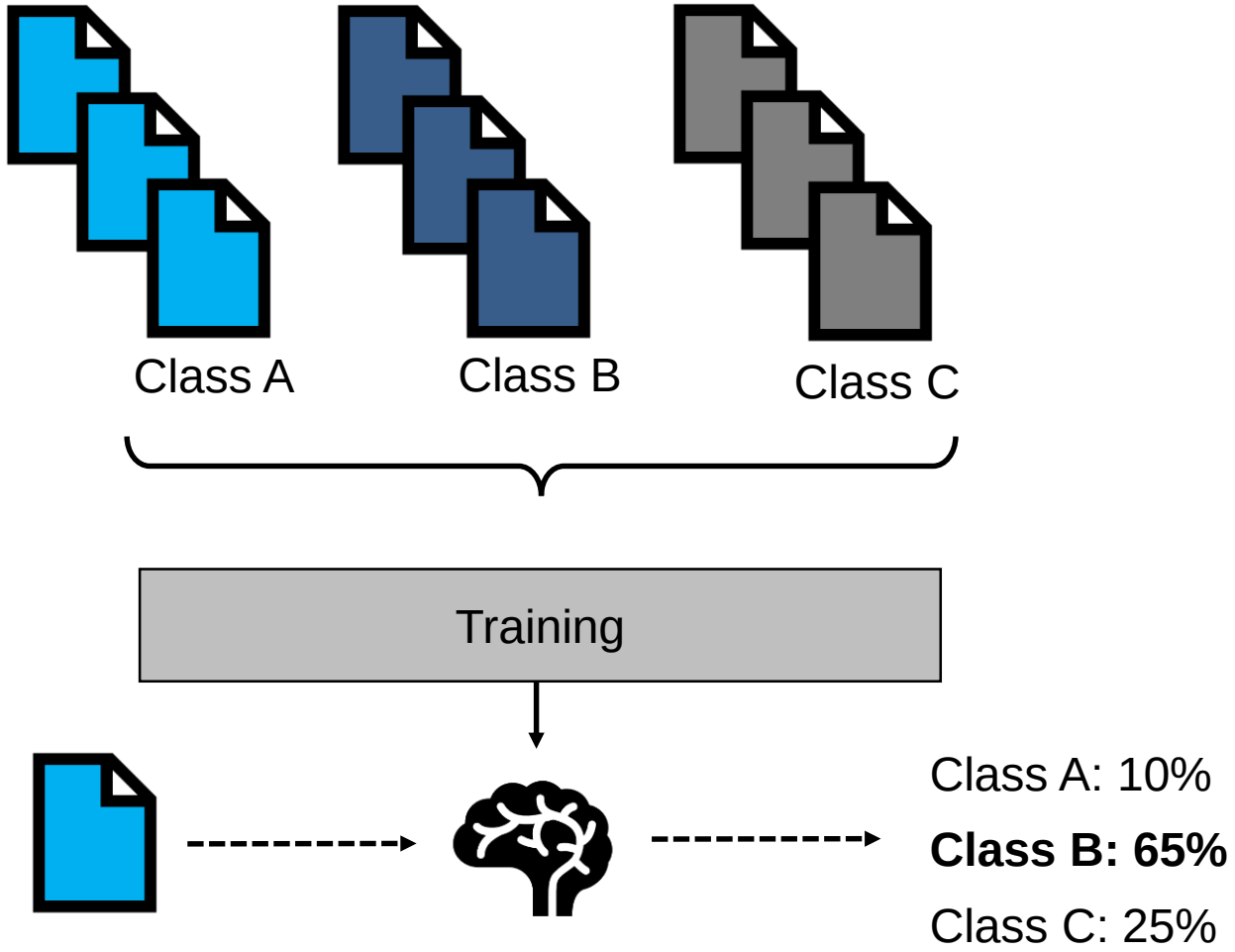
General Data Protection Regulation: Recital 162

- „ This Regulation should also apply to the processing of personal data for **statistical purposes**. […]“
- „[…] The term 'statistical purposes' means any **operation necessary for the performance of statistical investigations** and the production of statistical results. […]“
- „[…] These statistical results can be further **used for various purposes, including scientific research**. […]“
- „[…] In the context of statistical purposes, it is understood that the **results of processing for statistical purposes are not personal data** but aggregated data and that these results or personal data are not used for measures or decisions concerning individual natural persons. […]“

What Can Go Wrong? Types of Disclosure



What Can Go Wrong? Examples



Membership disclosure

- Input data that are classified by the model with high confidence are likely to be similar to training data

Attribute disclosure

- Model inversion: with known output, input values can be reconstructed

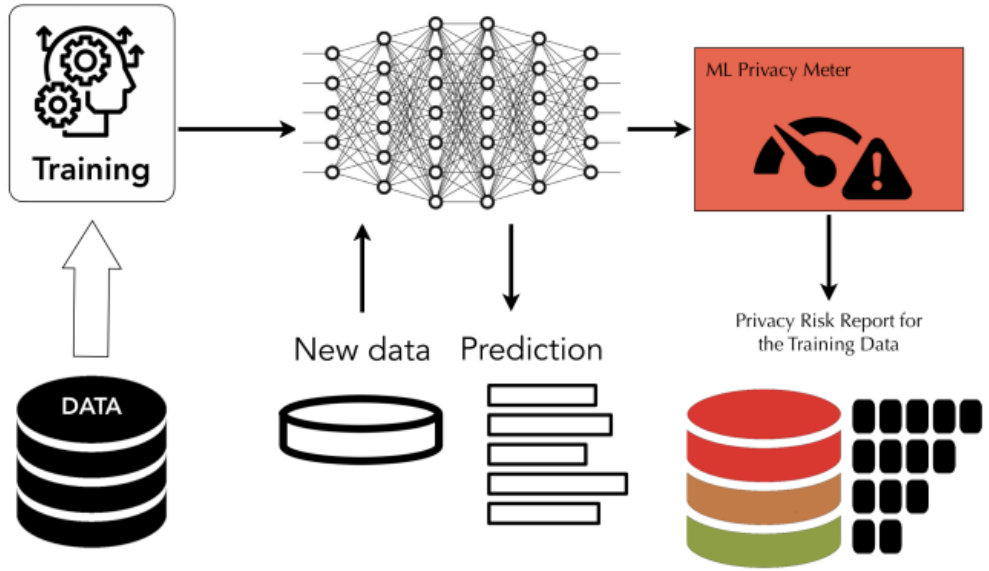
Data leaks

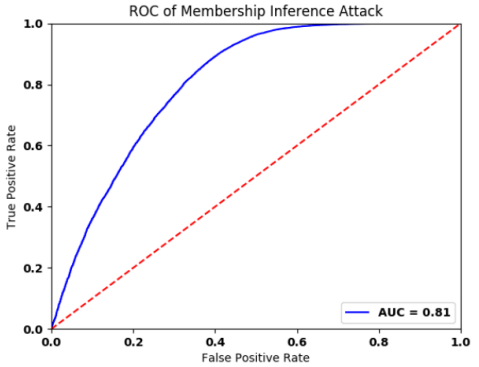
- For example, memorization by language models

Source: Shokri, R., Stronati, M., Song, C., & Shmatikov, V. (2017, May). Membership inference attacks against machine learning models. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 3-18). IEEE.

Privacy Tests

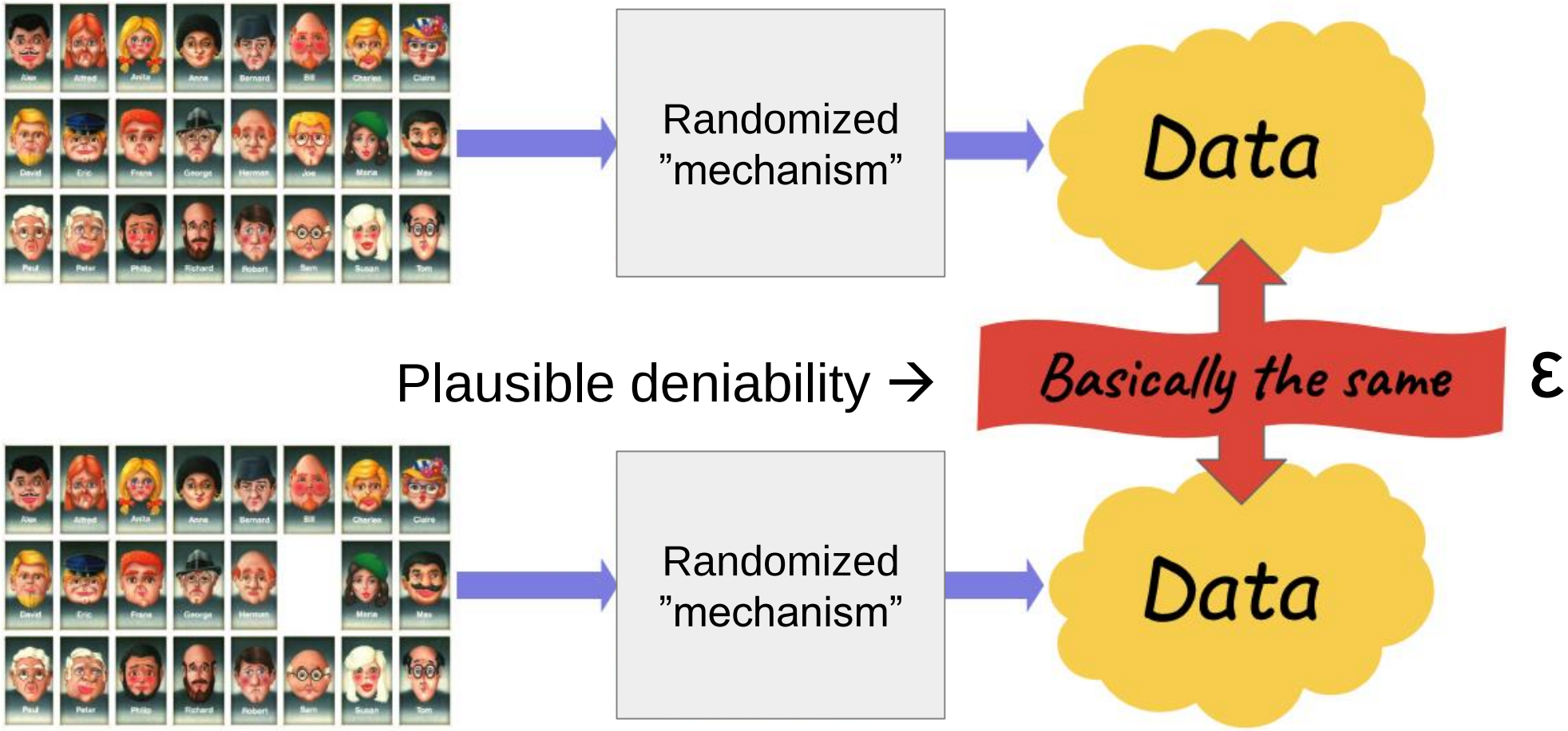
- Privacy tests evaluate whether a model leaks information about its training data, e.g. by allowing conclusions to be drawn about the presence of certain individuals
- For example, ML Privacy Meter examines confidence scores of predictions to identify patterns that could reveal the presence of training data
- What exactly is stored by LLMs is subject of ongoing research – downloading models fine-tuned on personal data is usually not permitted





Source: Murakonda, S. K., & Shokri, R. (2020). ML Privacy Meter: Aiding regulatory compliance by quantifying the privacy risks of machine learning. arXiv preprint arXiv:2007.09339.

Differential Privacy



Questions?

mi.bihealth.org