# CyberSec
# PII, Personal Data, and Regulations

**Tobias Sattler**
tobiassattler.com | cybersec.help

# Personal Identifiable Information (PII)

PII is used in the US but no federal law defines it.

Any **data** that could potentially be **used** to **identify** a specific **individual**.

PII can be divided into **2 categories**:

- **linked** information
- **linkable** information

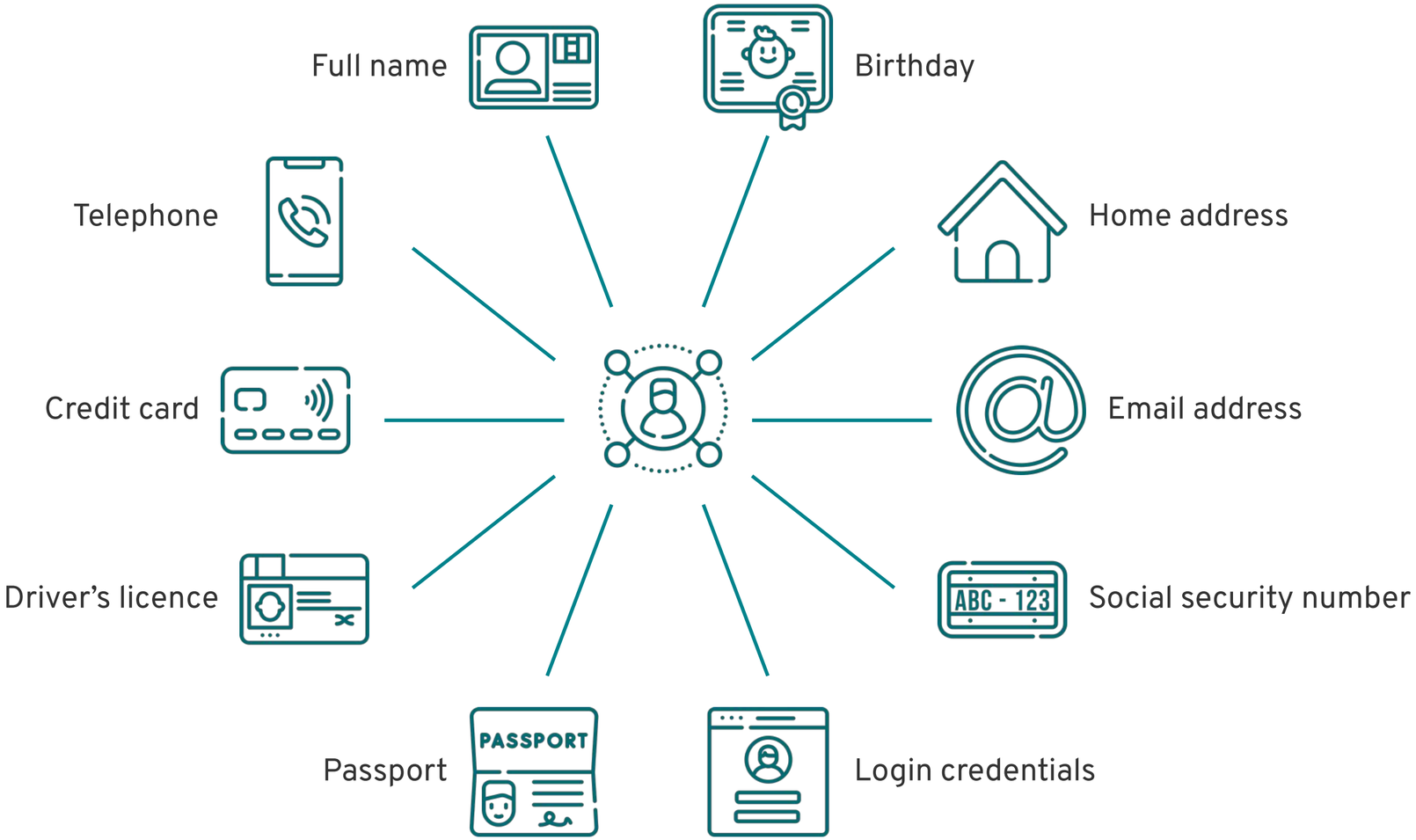
# National Institute of Standards and Technology definition

> *PII is **any information about** an **individual** maintained by an agency, including (1) any information that can be **used** to **distinguish** or **trace** an **individual's identity**, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any **other information** that is **linked** or **linkable** to an **individual**, such as medical, educational, financial, and employment information.*

Reference: NIST

# PII: Linked Information

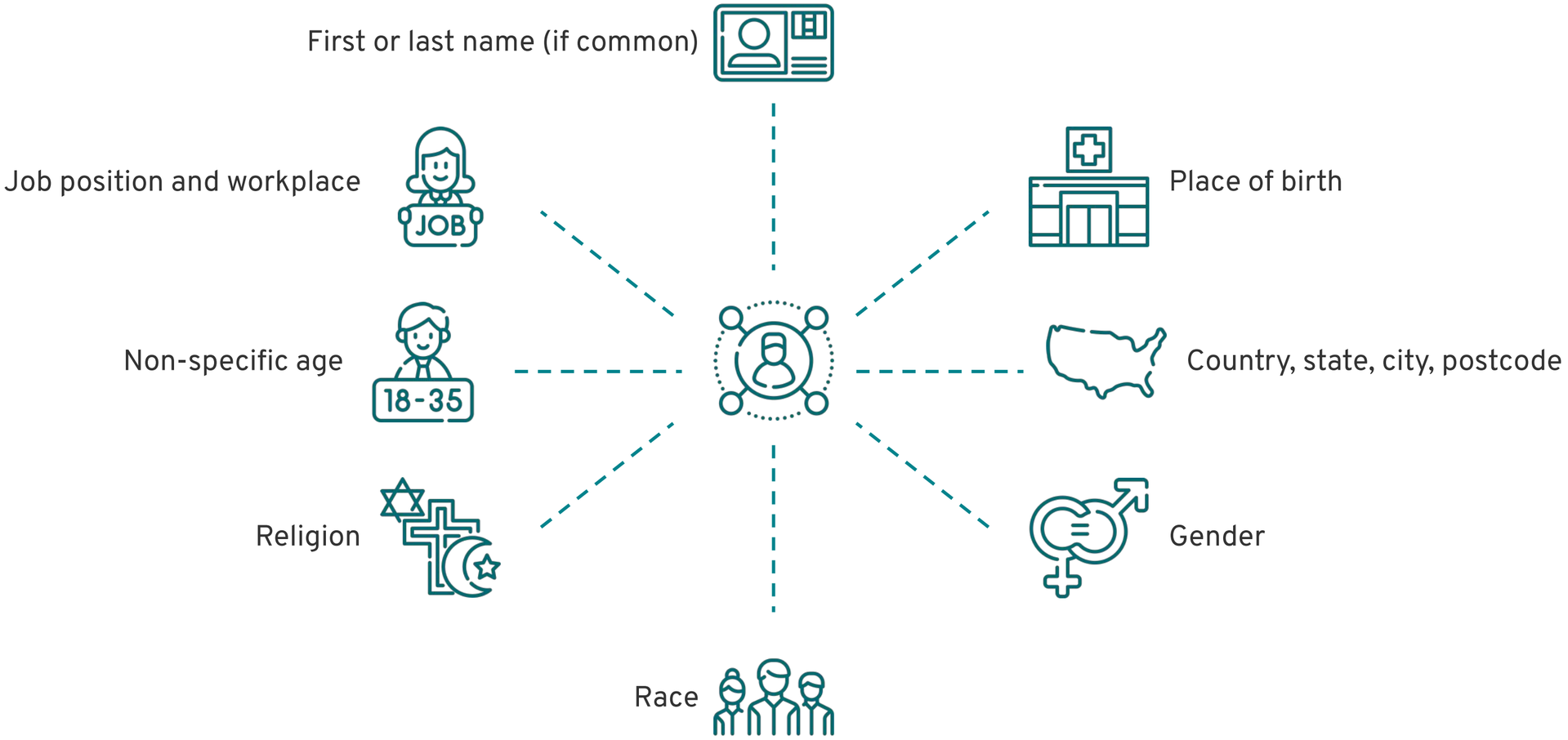
**Any piece** of personal information that can be **used** to **identify** an **individual** and includes, but is not limited to, the following:




This is only an illustration and does not claim to be exhaustive.

# PII: Linkable Information

**Information** that can **identify** a **person** when **combined** with **another piece** of information could identify, trace, or locate a person:




This is only an illustration and does not claim to be exhaustive.

# non-PII

**Data** that **cannot** be used **on its own** to trace, or identify a person.

**Classification** of PII and non-PII is **vague**. NIST doesn't reference cookie IDs and device IDs, others do.

Examples of non-PII include, but are not limited to

- **Aggregated statistics** on the use of product / service
- **Partially** or **fully masked** IP addresses

# Personal Data

**Defined by** the European General Data Protection Regulation (**GDPR**).

Covers a much **wider range** of information **than** personally identifiable information (**PII**).

**All PII** is considered **personal data**, not all personal data is PII.

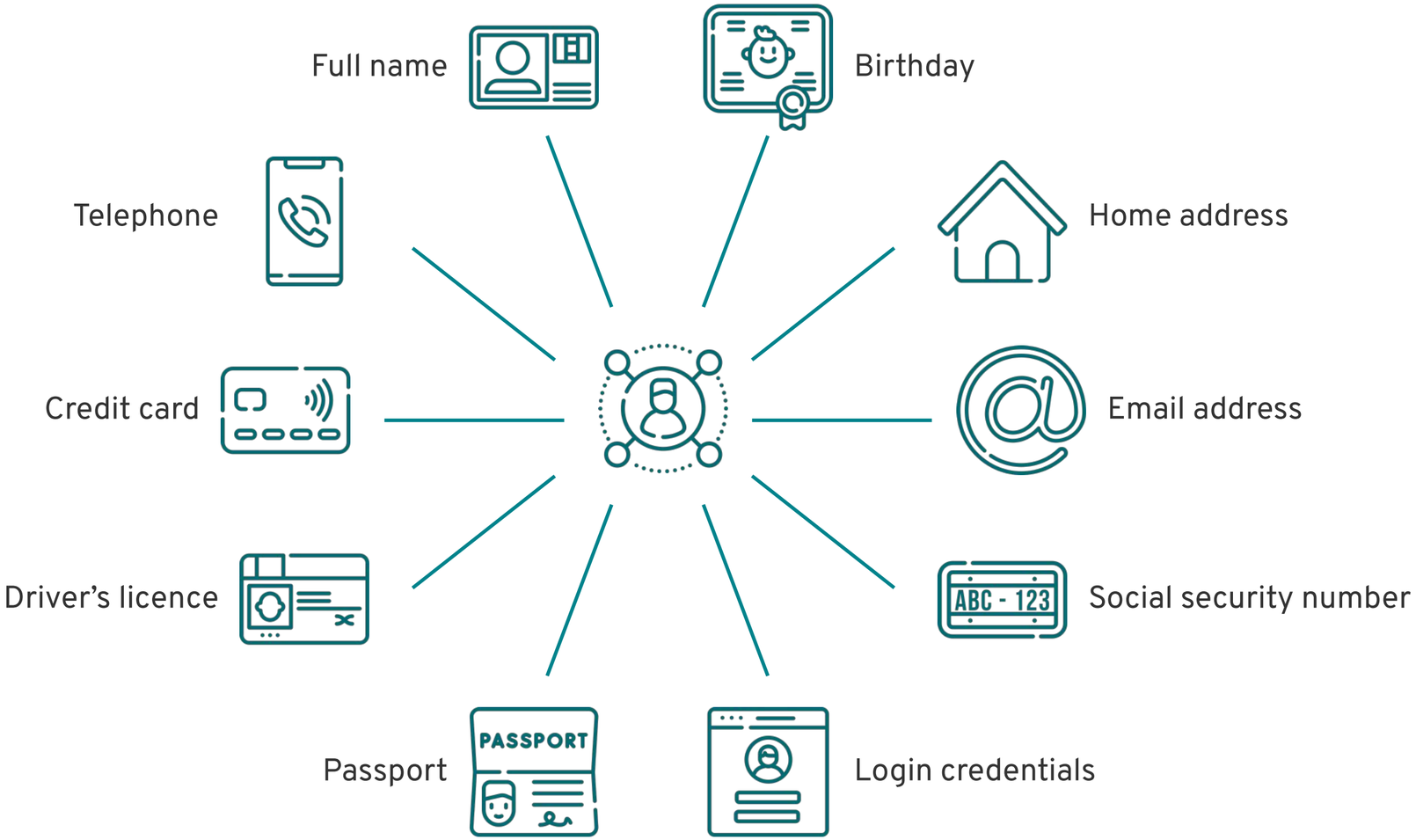
# GDPR Article 4 (1)

> “‘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;”

Reference: GDPR

# GDPR: Linked Information

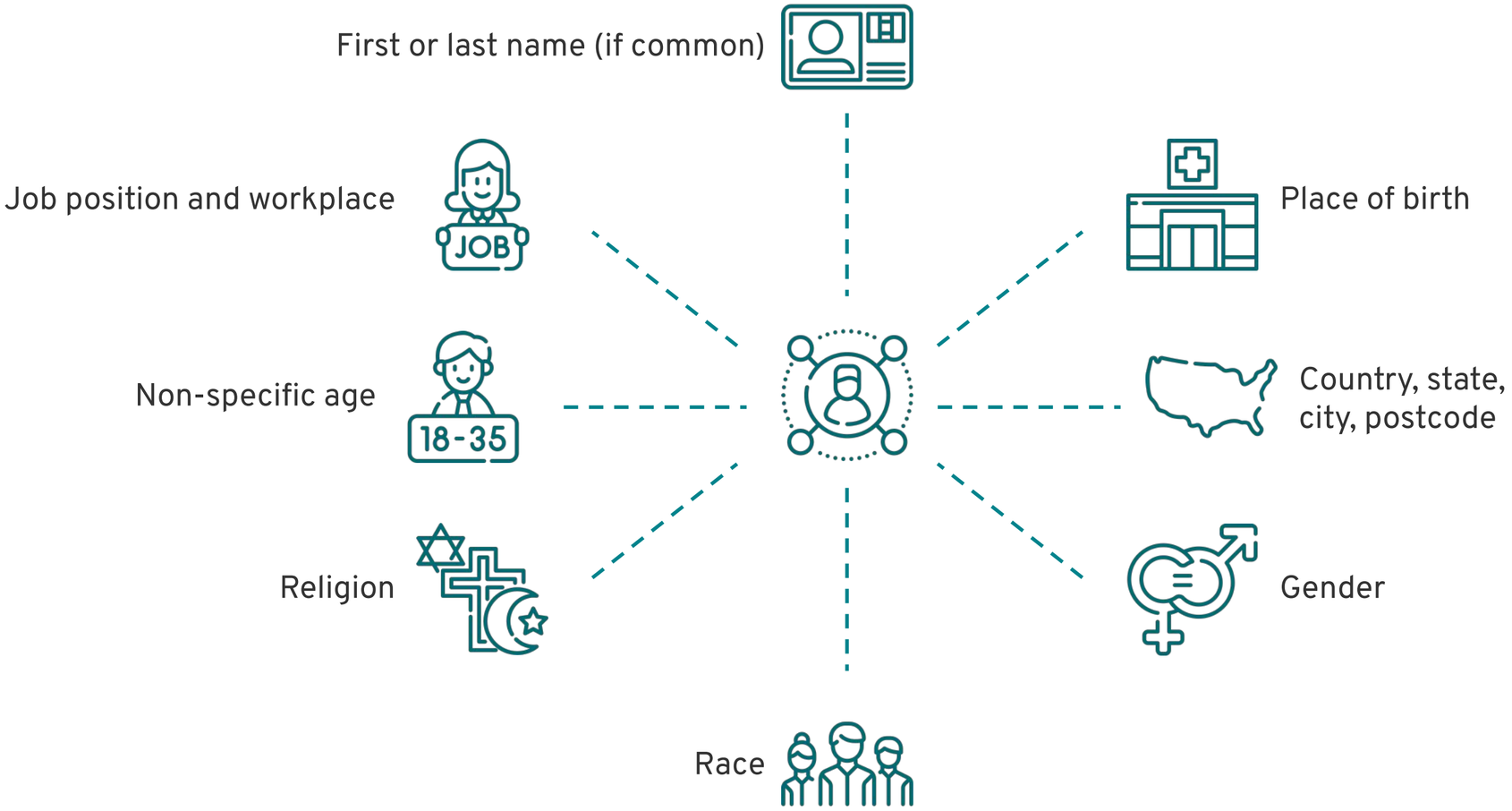
**Any piece** of personal information that can be **used** to **identify** an **individual** and includes, but is not limited to, the following:




This is only an illustration and does not claim to be exhaustive.

# GDPR: Linkable Information

**Information** that can **identify** a **person** when **combined** with **another piece** of information could identify, trace, or locate a person:




**Non-PII** data **but personal data** under GDPR:

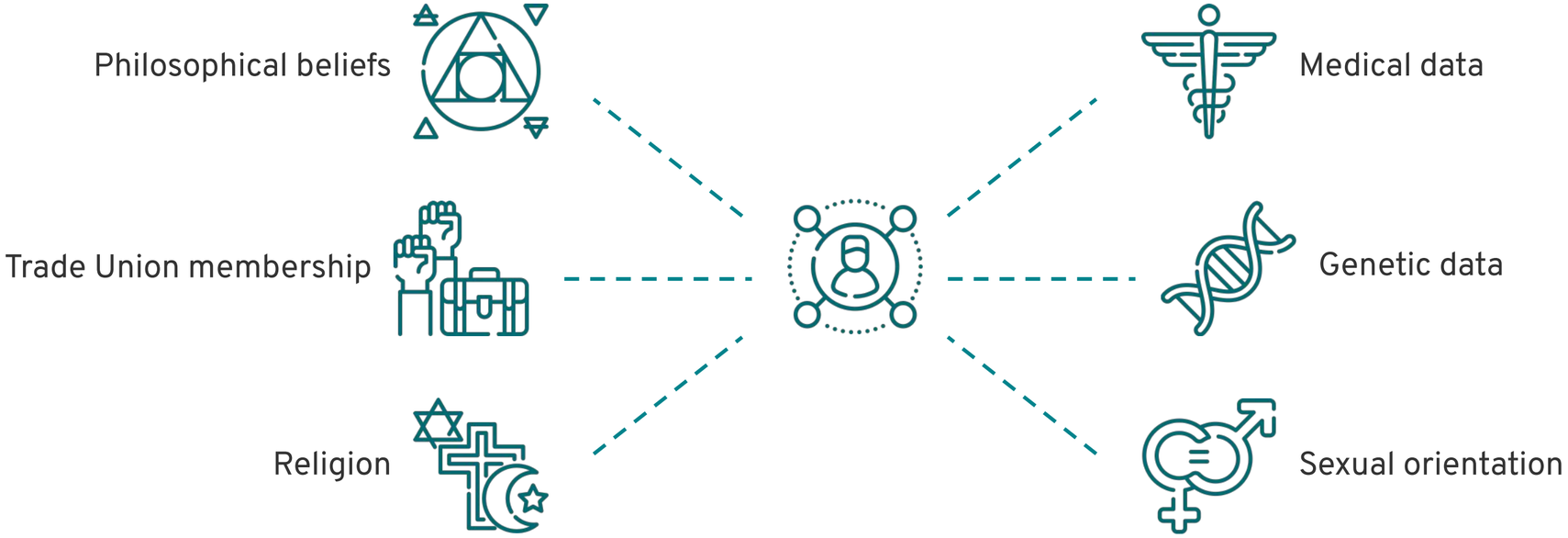
- Device ID
- IP address
- Cookies*
- Browser type*
- Plug-in details*

* depending on the context

This is only an illustration and does not claim to be exhaustive.

# GDPR: Sensitive Data

The **following** personal **data** are considered as **special** categories of personal data and are **subject** to specific processing conditions according to the **Article 9** of the GDPR. Processing is **generally prohibited** and only permitted under certain conditions.




This is only an illustration and does not claim to be exhaustive.

# non-Personal Data

Also **defined** in the **GDPR**, most simply as information that does not enable identification of an individual.

Examples of non-personal data include, but are not limited to

- **Aggregated statistics** on the use of product / service
- **Partially** or **fully masked** IP addresses
- **Anonymized** and **pseudonymized** data

# Data Regulation Policies #1

This extract shows some essential data regulation policies around the world.

| | |
|---|---|
| **CCPA** | The California Consumer Privacy Act (CCPA) is a **California** state privacy law that governs how companies worldwide may handle the personal information of California residents. The effective date of the CCPA is January 1, 2020, and it is the **first law** of its kind in the **United States**. |
| **FERPA** | The Family Educational Rights and Privacy Act (FERPA) of 1974 is a **United States** federal law that governs the access to **educational information** and records by public entities such as potential employers, publicly funded educational institutions, and foreign governments. |
| **GDPR** | The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy in the **European Union** (EU) and the European Economic Area (EEA) that came into effect on 25 May 2018—**regardless** of its **location** and the data subjects' **citizenship** or **residence**. |
| **HIPAA** | The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a **United States** federal statute that modernized **healthcare information** flow, stipulating how personally identifiable information should be protected from fraud and theft. |

# Data Regulation Policies #2

This extract shows some essential data regulation policies around the world.

| | |
|---|---|
| **HITECH** | The Health Information Technology for Economic and Clinical Health (HITECH) Act **added** several **provisions** that strengthen the civil and criminal enforcement of the **HIPAA** rules by adding categories of violations and tier levels of penalty amounts. |
| **LGPD** | The **Brazilian** General Data Protection Act (LGPD) of 2020 aims to unify 40 different Brazilian laws that regulate the processing of personal data. It is intended to protect personal data and strengthen Brazil's economy by **aligning with** international compliance standards set by **GDPR**. |
| **PCI-DSS** | The Payment Card Industry Data Security Standard (PCI-DSS) is an information security **standard** for organizations that handle **credit cards** from the major card schemes to reduce credit card fraud. |
| **PIPEDA** | The Personal Information Protection and Electronic Documents Act (PIPEDA) is a **Canadian** law relating to data privacy. It governs how private sector organizations collect, use and disclose personal information in commercial business. |

# Data Regulation Policies #3

This extract shows some essential data regulation policies around the world.

| | |
|---|---|
| **PIPL** | The **Chinese** Personal Information Protection Law (PIPL) came into take effect on November 1, 2021, and shares **many similarities** with the EU's **GDPR**, including its extraterritorial reach, restrictions on data transfer, compliance obligations, and sanctions for non-compliance. |
| **POPI** | The **South African** Protection of Personal Information (POPI) Act focuses on data privacy **inspired** by other foreign national treaties like the **United Kingdom**. |

# Thank you!

**See more on cybersec.help**

References: (1) Icons made by Freepik (2) Cover made by TheDigitalArtist