inventeurs du monde numérique

GDPR and research

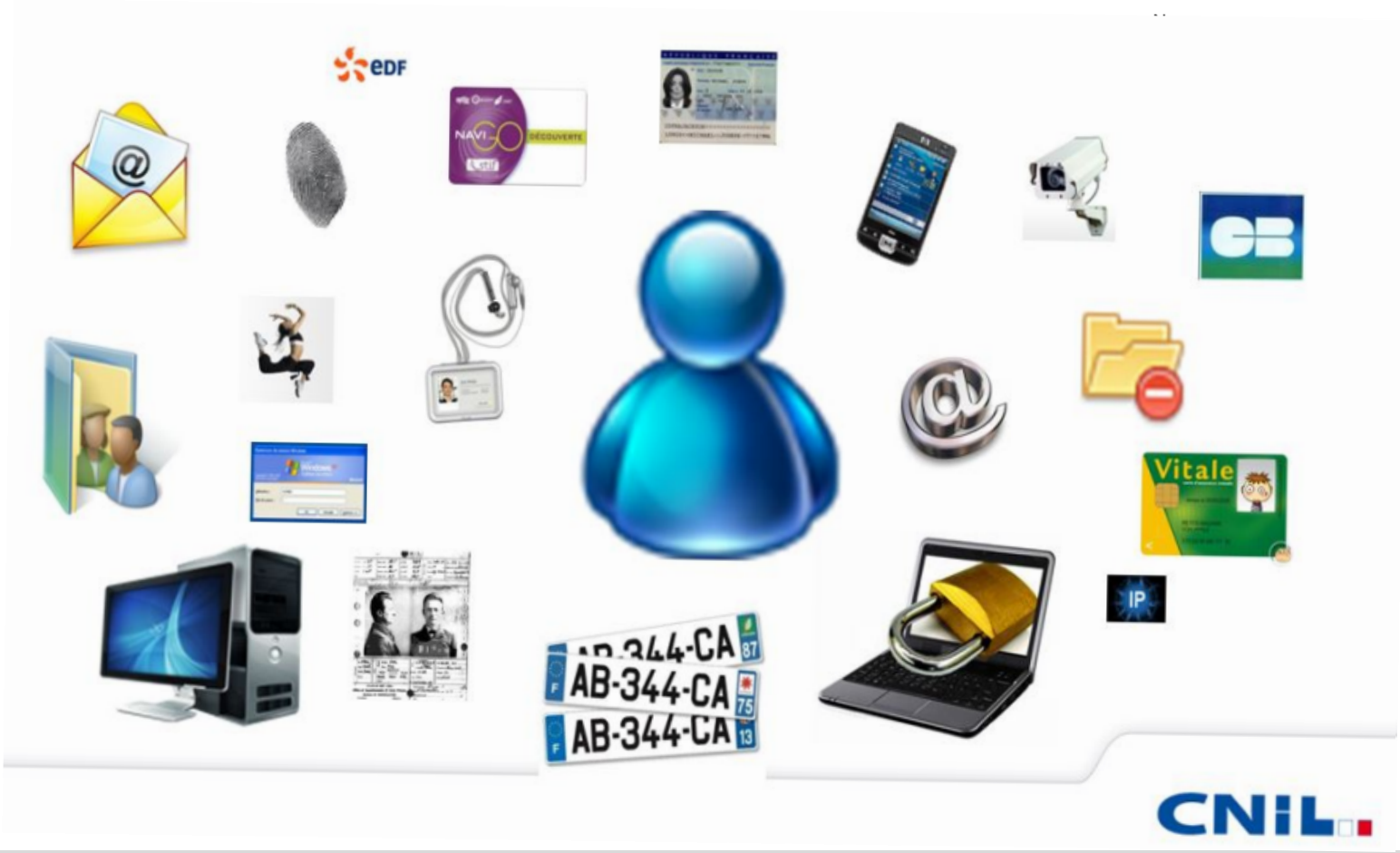
GDPR

What is GDPR?

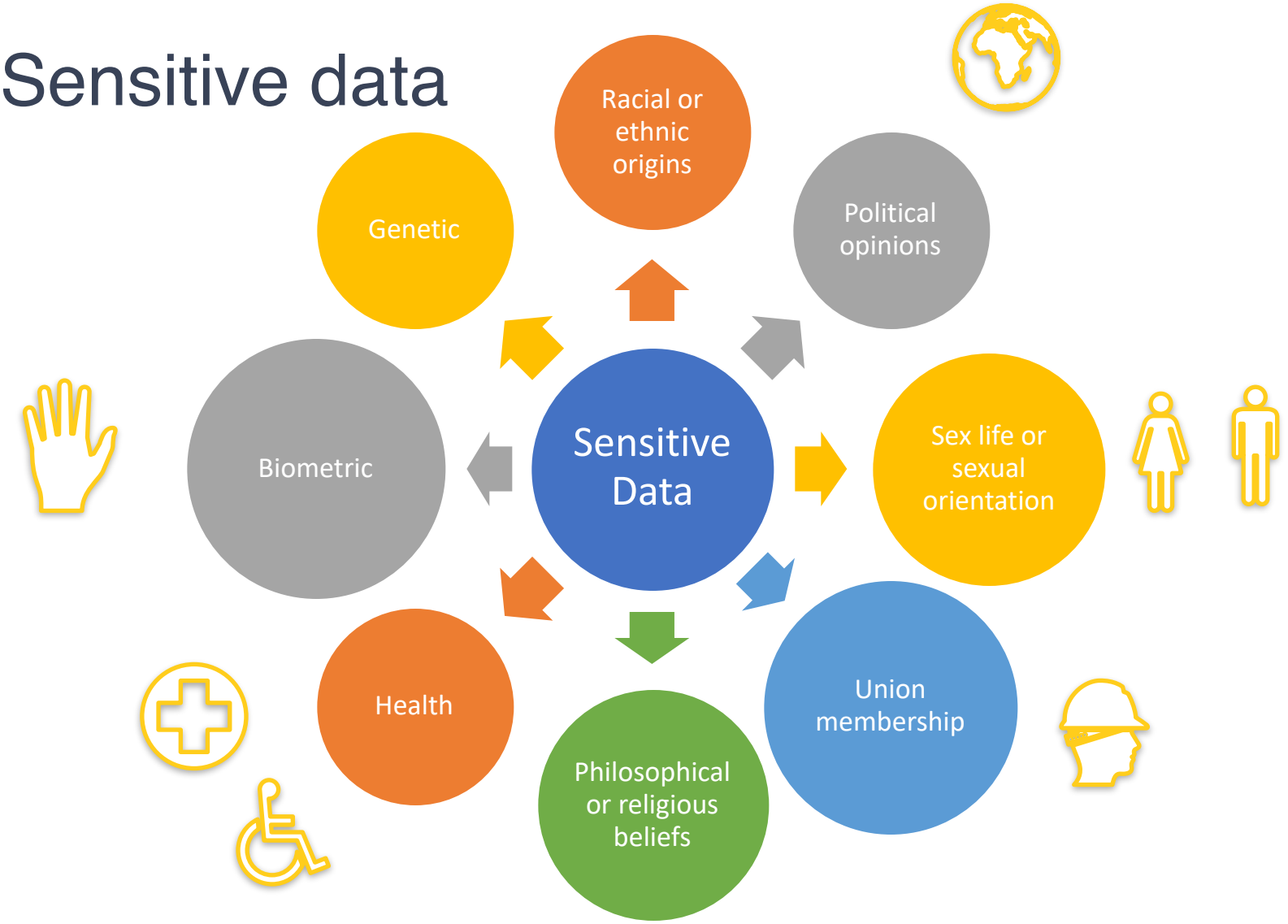
1. GDPR

Some definitions

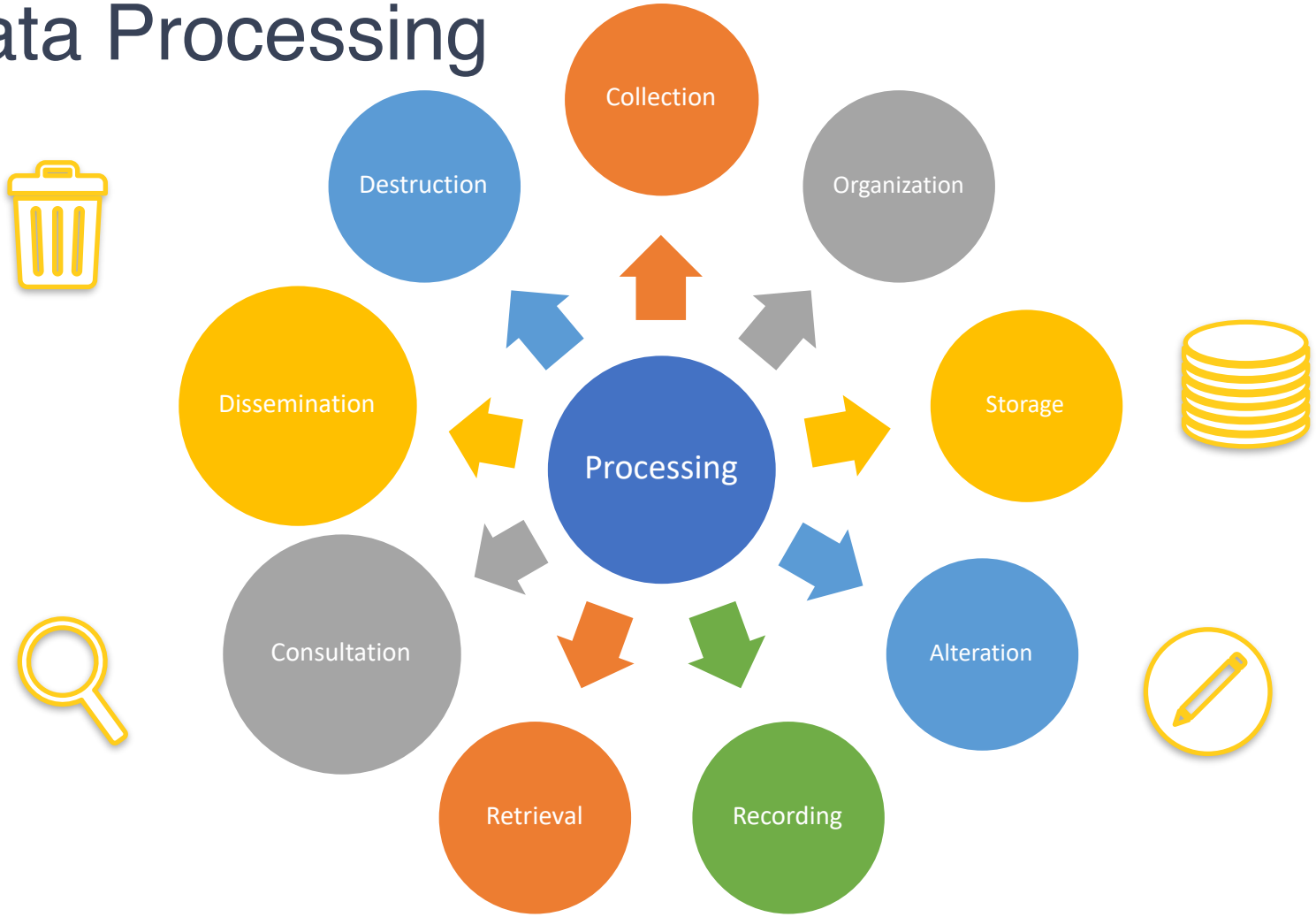
Personal Data



Sensitive data



Data Processing



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;

Controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing** of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Processor

A natural or legal person, public authority, agency or other body **which processes personal data on behalf of the data controller**;

Personal Data Breach

A breach of security leading to the accidental or unlawful **destruction, loss, alteration, unauthorised disclosure of, or access to, personal data** transmitted, stored or otherwise processed;

1. GDPR

What is GDPR?

What is GDPR?

GDPR

- data protection reglementation which applies to all European Union (EU) countries from 25 May 2018
- concerns personal data
- Applies to a company
  - which processes personal data as part of the activities of one of its branches established in the EU, regardless of where the data is processed;
  - established outside the EU offering goods/services (paid or for free) or monitoring the behaviour of individuals in the EU.

Actors

- Supervisory Authority (In France : CNIL)
- Data Protection Officer
- Controller / Processor
- Data subject

2. GDPR

Changes with GDPR

Shared responsibilities

Controller

Determines the purposes and means of the processing

- **GDPR increases in its obligations**

Processor

processes personal data on behalf of the controller

- **GDPR standardizes its obligations with those of the controller**

Joint controllers

the 2 controllers define their respective obligations in a transparent manner

- **New with GDPR**

GDPR strengthens obligations for organizations

From the beginning and throughout the life of the project

Implementation of a real policy for the governance of personal data

Accountability ability of the controller/processor to demonstrate compliance at any time

Privacy by design the controller implements... appropriate technical and organizational measures, such as pseudonymization, which are intended to implement data protection principles... in order to protect the rights of the data subject.

Privacy by default the controller shall implement appropriate technical and organizational measures to ensure that, by default, only those personal data which are necessary for each specific purpose of the processing operation are processed

Exercise of the rights of data subjects whenever personal data is collected

GDPR strengthens the rights of the data subjects

Transparency

Information to the data subjects

- concise, understandable
- easily accessible
- in clear and simple terms

Enhanced consent

The data subjects

- be informed of the use of their data
- give their agreement to the processing of their data
  accountability

Rights of rectification & erasure

Data subjects may exercise their rights of rectification or erasure at any time

Right of opposition & automated individual decision-making

The data subjects may exercise their right to object at any time.

Data subjects have the right not to be the subject of a decision based exclusively on automated processing, including profiling

GDPR Compliance Tools

A Data Protection Officer (DPO) ✔

- An obligation for public authorities or organizations

Register of processing ✔

- It contains the different processing operations and their management: who is responsible for the processing, is it sensitive data, where the data are hosted, how long they are kept, their purpose

Notification of personal data breach (to authorities and individuals concerned) ✔

- Obligation for the controller to report to the authorities within 72 hours of the violation of personal data. Information to data subjects if the violation is likely to create a high risk to their rights and freedoms

Privacy Impact Assessments (PIA) ✔

- For high-risk processings, a data protection impact assessment should be carried out by the controller (need for data security, risks and measures adopted)

GDPR strengthens sanctions

To have a DPO doesn't prove the compliance to GDPR

Administrative sanctions in case of non-compliance with the provisions of the Regulation:

- Warning
- Order
- Temporary or permanent limitation of processing
- Suspension of data flows
- Correction, limitation or deletion of data

Financial sanctions : de 10 à 20 millions d'euros (for a public organization)

Main risk pour Inria : damage to brand image and reputation

GDPR

How to apply GDPR to a scientific experiment using personal data?

1 - Responsibility / Purpose / Legal basis / Data

Responsibility

- Controller / Processor / Joint Controller

Purpose of processing

- Personal data contained in a processing operation shall only be collected and processed for a **determined and legitimate use, previously defined**

Lawful basis of processing

- Consent / Performance of public interest / Performance of contract

Data

- **Privacy by default**
- **Data retention** : The data must be kept only for as long as necessary for the fulfillment of the purposes of the processing operation
- Who will have **read / write access to the data**?

2 - Privacy Impact and Ethics

Privacy Impact Assessment (PIA) with Inria sensitivity scale

1. Evaluate impacts for data subjects if data is **Unavailable / Modified fraudulently / Published on Internet**
   - **Null / Moderate / Significant / Catastrophic**
2. Deduce from the impacts the Sensitivity level of the data
   - **Public / Limited diffusion / Confidential / Restricted information**
3. Choose the application to store and exchange data, according to the trust in the provider
   - Ex1: Public data -> Dropbox, Google, Amazon, etc.
   - Ex2: Limited diffusion -> partage.inria.fr or mybox.inria.fr
   - Ex3: Confidential data -> mybox.inria.fr with encrypted folders

If the experiment uses sensitive data *(health data, social networks, etc.)*

- Implement the Ethical Committee of Inria (COERLE) recommendations
- Fill the COERLE form and submit it to the COERLE decision
- **If health data**
  - The hospital submits the experiment to a CPP (Committee for the Protection of Persons
  - Apply reference methodology : MR001, MR002, etc.

3 - Rights of Data Subjects and Data Transfers

Rights of data subjects

- Implement transparency rules
  - How data subjects
    - will be informed?
    - will give their consent?
      - Consent form for health data
  - How the requests for the exercise of rights will be processed?

Data transfers outside of Europe

- Check if country has an adequate level of protection of personal data
  - If yes, the transfer is ok
  - If no
    - Use standard contractual clauses approved by the European Commission
    - The individual must explicitly consent to the transfer after having been informed about the risks associated with the transfer

4 - Inform / Implement security measures / Document

Send a mail to the lawyer of Centre and to the DPO dpo@inria.fr

- DPO will organize a meeting to check the compliance to GDPR of the experiment

Fill and send the declaration form of the experiment to dpo@inria.fr

- DPO will use it to complete the register of processing

Implement the technical and organizational measures for the compliance to GDPR

- Encryption / Pseudonomization / Access control
- Data isolation / Archiving

Keep documents to demonstrate the compliance to GDPR

- Emails
- Consent forms
- Keep and secure the tables used for pseudonomization
- Private Impact Assessment
- COERLE decision

Right Reflexes

If your are informed about

A personal Data Breach

- **Send immediately a mail to dpo@inria.fr**

A wish to exercise or right

- **Send immediately a mail to dpo@inria.fr**

A non compliance to GDPR

- **Send immediately a mail to dpo@inria.fr**

Thank you

Anne Combe - Data Protection Officer

Direction Générale

Inria
inventeurs du monde numérique