

# General Data Protection Regulation

Nataliia Bielova

[@nataliabelova](https://twitter.com/nataliabelova)

Security and ethical aspects of data

Université Cote d'Azur



# **GENERAL DATA PROTECTION REGULATION**

## TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

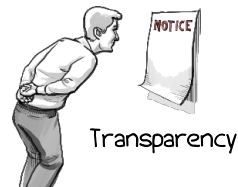
## LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

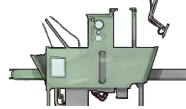


## RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



"Right not to be subject to a decision based solely on automated processing, including profiling."

Access and Rectification



Right to Erasure

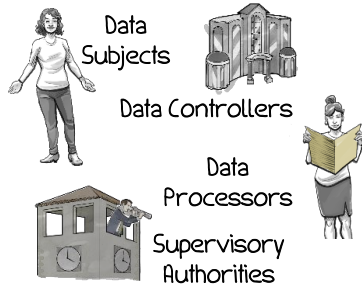


Purpose Specification and Minimization



Right to Data Portability

## THE PLAYERS

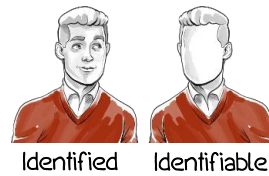


EU Establishments

Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

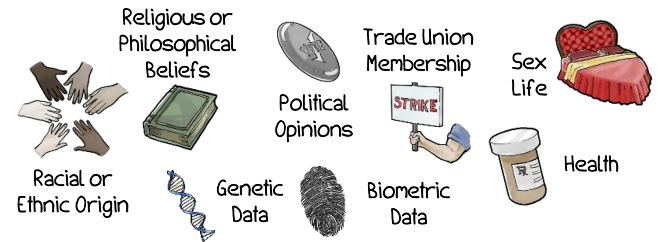
## PERSONAL DATA



Identified

Identifiable

## SENSITIVE DATA



## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security



Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.



Record of Data Processing Activities

Maintain a documented register of all activities involving processing of EU personal data.



Data Impact Assessment

For high risk situations

Data Protection by Design

built in starting at the beginning of the design process



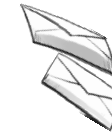
## CONSENT



Consent must be freely given, specific, informed, and unambiguous.

# GDPR

## DATA BREACH NOTIFICATION

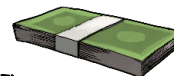


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

## ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.



Effective Judicial Remedies: compensation for material and non-material harm.



## INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection

Binding Corporate Rules (BCRs)



Privacy Shield



Model Contractual Clauses

## TERRITORIAL SCOPE

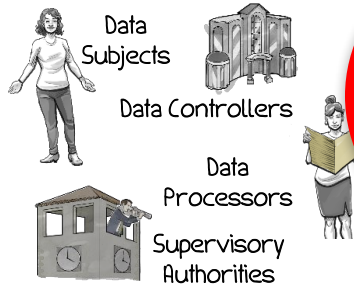


EU Establishments

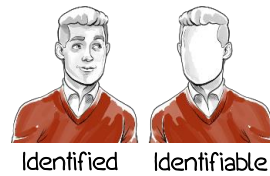
Non-EU Established Organizations

Offer goods or services or engaging in monitoring within the EU.

## THE PLAYERS

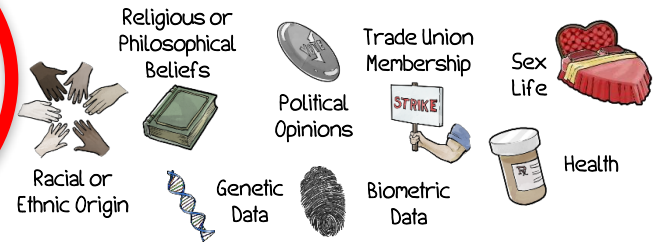


## PERSONAL DATA



Identified      Identifiable

## SENSITIVE DATA



## LAWFUL PROCESSING

Collection and processing of personal data must be for "specified, explicit and legitimate purposes" – with consent of data subject or necessary for

- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests

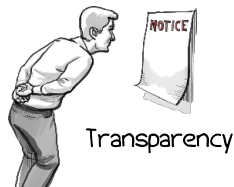


## CONSENT



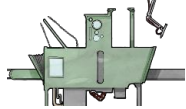
Consent must be freely given, specific, informed, and unambiguous.

## RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



"Right not to be subject to a decision based solely on automated processing, including profiling."

Access and Rectification



Right to Erasure



Purpose Specification and Minimization



Right to Data Portability



## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security



Data Protection Officer (DPO)

Designate DPO if core activity involves regular monitoring or processing large quantities of personal data.

Record of Data Processing Activities



Maintain a documented register of all activities involving processing of EU personal data.



Data Impact Assessment

For high risk situations

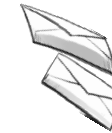
Data Protection by Design

built in starting at the beginning of the design process



# GDPR

## DATA BREACH NOTIFICATION

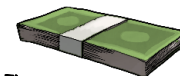


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

If likely to result in a high privacy risk → notify data subjects

Notify supervisory authorities no later than 72 hours after discovery.

## ENFORCEMENT



Fines

Up to 20 million euros or 4% of total annual worldwide turnover. Less serious violations: Up to 10 million euros or 2% of total annual worldwide turnover.



Effective Judicial Remedies: compensation for material and non-material harm.



Binding Corporate Rules (BCRs)



Adequate Level of Data Protection



Privacy Shield



Model Contractual Clauses



# PERSONAL DATA

## Art. 4 GDPR

# Definitions

‘**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;

<https://gdpr-info.eu/art-4-gdpr/>



## **ANY INFORMATION**

Objective (earns 10k per year); Subjective (opinion); and, Sensitive data (gay woman).



## **RELATING TO**

An individual, about a particular person, impacts a specific person.



## **IDENTIFIED OR IDENTIFIABLE**

Direct or indirectly e.g. You know me by name, direct, you know me as "a Lawyer doing these graphics", indirect.



## **NATURAL PERSON**

applies ONLY to a living human being. National Law may give rules for deceased persons.



## **ONLINE IDENTIFIER & LOCATION DATA**

Include data provided by the electronic devices we use: mobiles, cookies identifiers, IP address, others.



## **TO ONE OR MORE FACTORS**

Include data that when combined with unique identifiers and other info create a profile and identify a person.



# 1. Any information can be personal data



- Any information can fall under personal data **regardless** of its **nature, content, or format**:
  - **Nature**: true or inaccurate, objective and subjective (including opinions and assessments) [Nowak, 2017]
  - **Content**: not strict to private or family life, and could concern an individual's professional life, and other capacities
  - **Format**: **alphabetical**, numerical, graphical, photographic or acoustic, kept on paper or stored in a computer memory as a binary code, structured or unstructured, **video and voice recording**, as well as a child's drawing that could contain personal data of both the child and the parents





## 2. Relating to

- Any information can “relate” to a person in 3 conditions: **content, purpose, or result** (not cumulative)
  - 1. Content:** facts **about** that person’s identity, characteristics or behaviour [YS and others,2016]

eg. medical, criminal, professional, sporting achievements record; personal bank statements; itemised telephone bills
  - 2. Purpose:** when data are used, or *are likely to be used*, with the purpose to evaluate, treat in a certain way, influence the status or behaviour of an individual, make a **decision** about him

eg. a person carried unauthorized alterations to their house. The data about the unauthorized alterations is processed by reference to the house address. If this data is processed in order to decide whether to prosecute the house owner, the data relates to him
  - 3. Result/Impact:** when its use is likely to have an impact on a person’s **rights and interests’**

eg. different treatment; intended or accidental/ unpredictable (ML algorithms and data analytics)  
eg. information recorded to monitor the productivity of an employee who operates a machine; the annual bonus depends on achieving a certain level of productivity, and so, the information will be personal data about that individual employee who operates it



# 3. Identified or Identifiable (1)



§26, 30 WP136

- **Identified:** person who is known, or distinguished from the others in a group
- **Identifiable:** person who is not identified yet, but identification is possible
- **Directly:** reference to a name, in combination with additional information, if the name is not unique  
eg. [johnsmith@example.com](mailto:johnsmith@example.com), “elderly man lives at nr 15 Purple St and drives a Porsche”, “Maria’s foster mum, from Year 4 at Junior School”
- **Indirectly:** unique combinations of indirect identifiers that allow a person to be singled out from others  
eg. car registration number, combination of significant criteria (age, occupation, place of residence)

Online Identifiers
IP address
Cookies
RFID Tags
MAC addresses
Advertising IDs
Account usernames
Device fingerprints

Direct Identifiers	Indirect Identifiers
Name	Physical
Address details	Physiological
Email address	Genetic
ID number	Mental
Location data	Economic
	Cultural
	Social Identity

# HOW COMPANIES IDENTIFY PEOPLE

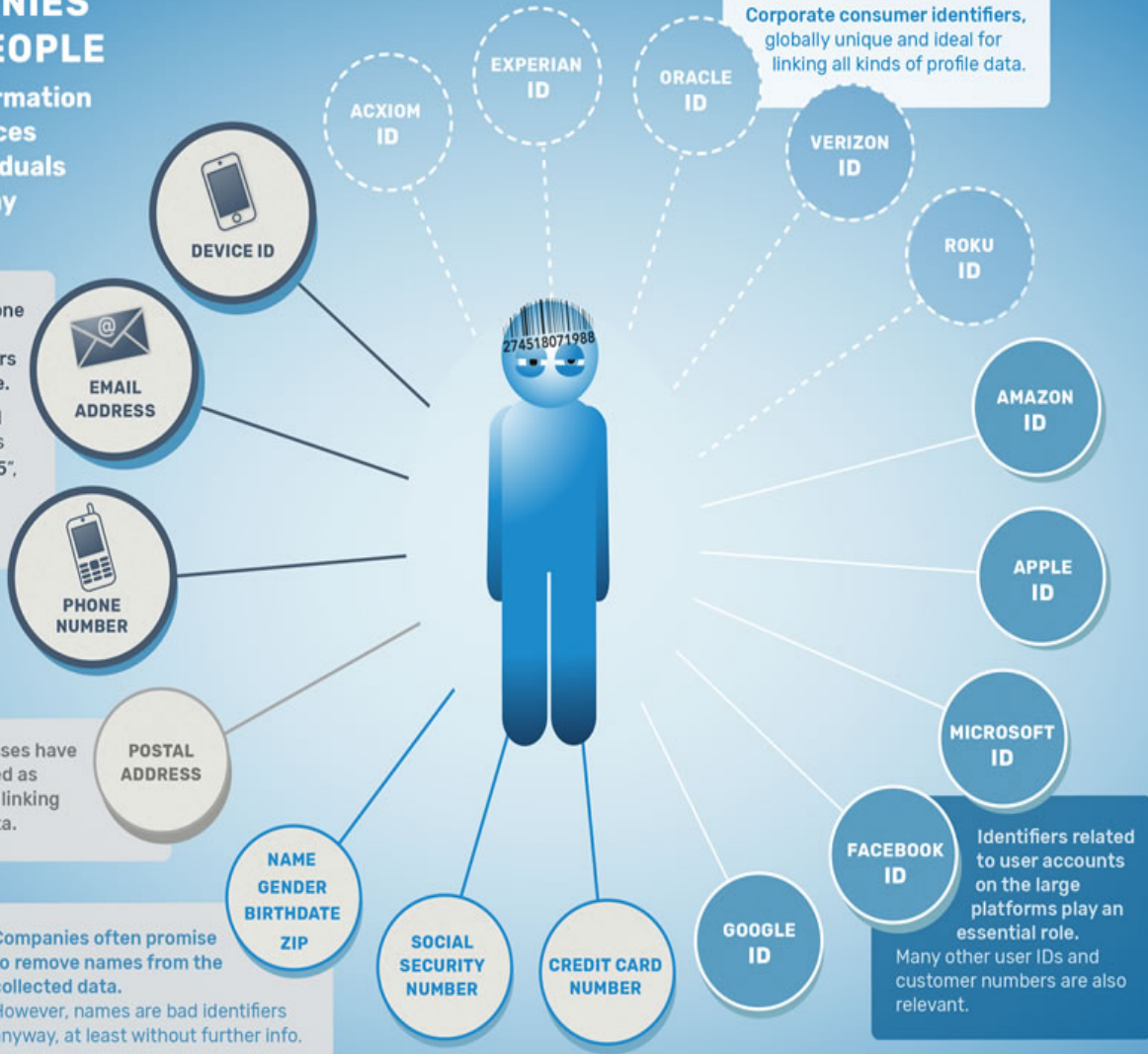
to link profile information from various sources and monitor individuals throughout the day

Email addresses and phone numbers are among the most important identifiers used to recognize people. They are often converted into pseudonyms such as "e907c95ef289bxw2345", which can still serve as personal ID numbers.

Postal addresses have long been used as key nodes for linking consumer data.

Companies often promise to remove names from the collected data. However, names are bad identifiers anyway, at least without further info.

Corporate consumer identifiers, globally unique and ideal for linking all kinds of profile data.



Many other kinds of temporary identifiers are used to track people across websites, platforms and devices:

People can also be (re)identified through calculating digital fingerprints from behavioral data:



## 2. Test of “reasonably likelihood” of identification



§26 WP136

To check if a person is identifiable, account to be taken to:

- All **means** “**reasonably likely**” to be used to identify an individual, directly or indirectly
  - eg. public registry, reverse directory
- By any person (not necessary that all the information to identify must be in the hands of one person [Breyer, 2016])
  - eg. ordinary person or by a particular person: investigative journalists, ex-partner, stalker, industrial spies

### Objective factors:

- Cost/time needed for identification, in light of new technology, security developments, or changes to the public availability of certain records
- Intended explicit or implied purpose of processing
- Available tools for identification
- Risk of organizational dysfunctions, eg. breaches of confidentiality duties, technical failures
- State of the art of technology at the time of processing, and technological developments



# Examples of personal data

Company uses WiFi analytics data to count the nº of visitors/hour across different retail outlets. It processes a person's Media Access Control address (MAC) through the public WiFi hotspots. If an individual can be identified from his MAC address device, or with other information in the possession of this business, then the data is personal data



# Examples of personal data

Using cookies, or similar technologies, to track people across websites, consists in processing of personal data (specially if this tracking involves online identifiers used to create a profile of a person)



# Examples of personal data

An individual submits a job application. The HR department removed the first page containing the individual's name, contact details, etc and saves the remainder of the form in 'Folder 1' and sent the rest on to the recruiting manager. The information in Folder 1 does not allow for the identification of any individual, but when it is combined with the second part, the applicant can be identified