UNIVERSITÉ CÔTE D'AZUR

Inria INVENTEURS DU MONDE NUMÉRIQUE

General Data Protection Regulation

Nataliia Bielova

@nataliabielova

Privacy, Security and ethical aspects of data

Université Cote d'Azur

GENERAL DATA PROTECTION REGULATION

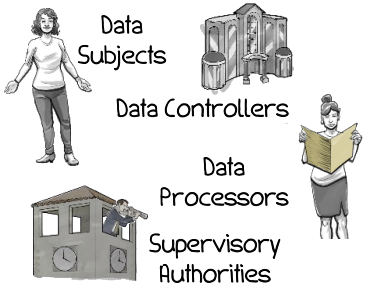
GDPR

TERRITORIAL SCOPE

EU Establishments

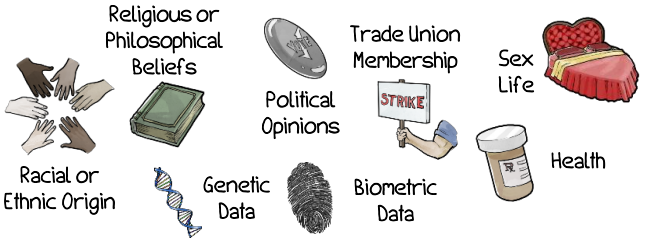
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



PERSONAL DATA

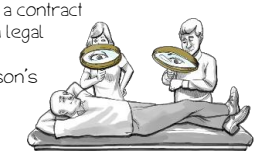
SENSITIVE DATA



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



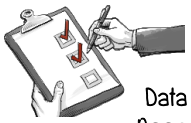
CONSENT

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

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

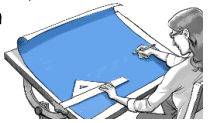
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

Record of Data Processing Activities
Maintain a documented register of all activities involving processing of EU personal data.

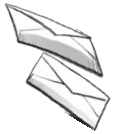


Data Impact Assessment
For high risk situations

Data Protection by Design
built in starting at the beginning of the design process



DATA BREACH NOTIFICATION

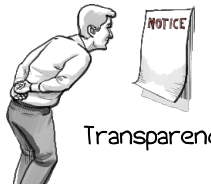


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making

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

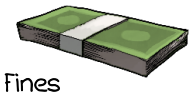
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

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

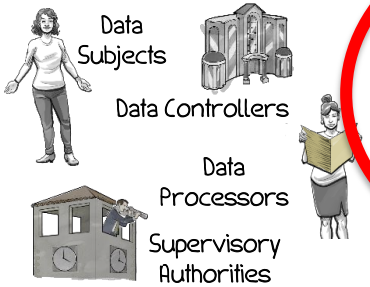
GDPR

TERRITORIAL SCOPE

EU Establishments

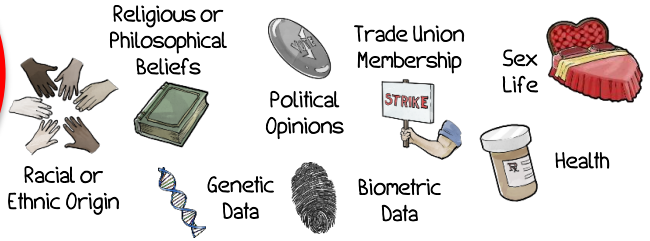
Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS

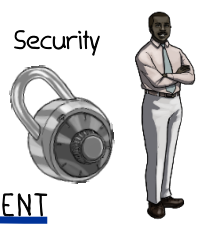


PERSONAL DATA

SENSITIVE DATA

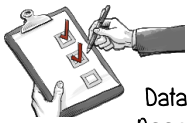


RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS



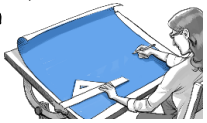
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

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

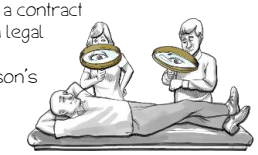
Data Protection by Design
built in starting at the beginning of the design process



LAWFUL PROCESSING

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

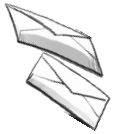
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

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

DATA BREACH NOTIFICATION

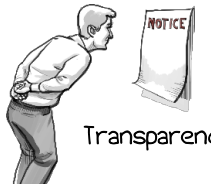


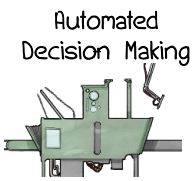
A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS





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

ENFORCEMENT

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

TEACHPRIVACY 2019
www.teachprivacy.com
Workforce awareness training by Prof. Daniel J. Solove

PERSONAL DATA

Slides of Cristiana Santos

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.

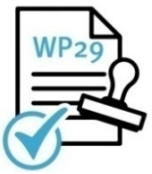
ONLINE IDENTIFIER & LOCATION DATA

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.

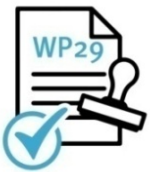
Slides of Cristiana Santos



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, photographical 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

Slides of Cristiana Santos



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

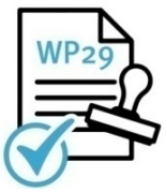
2. **Purpose:** when data are used, or *are likely to be used*, with the purpose to evaluate, treat in a certain way, influence the status or behaviour of an individual, make a **decision** about him

   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

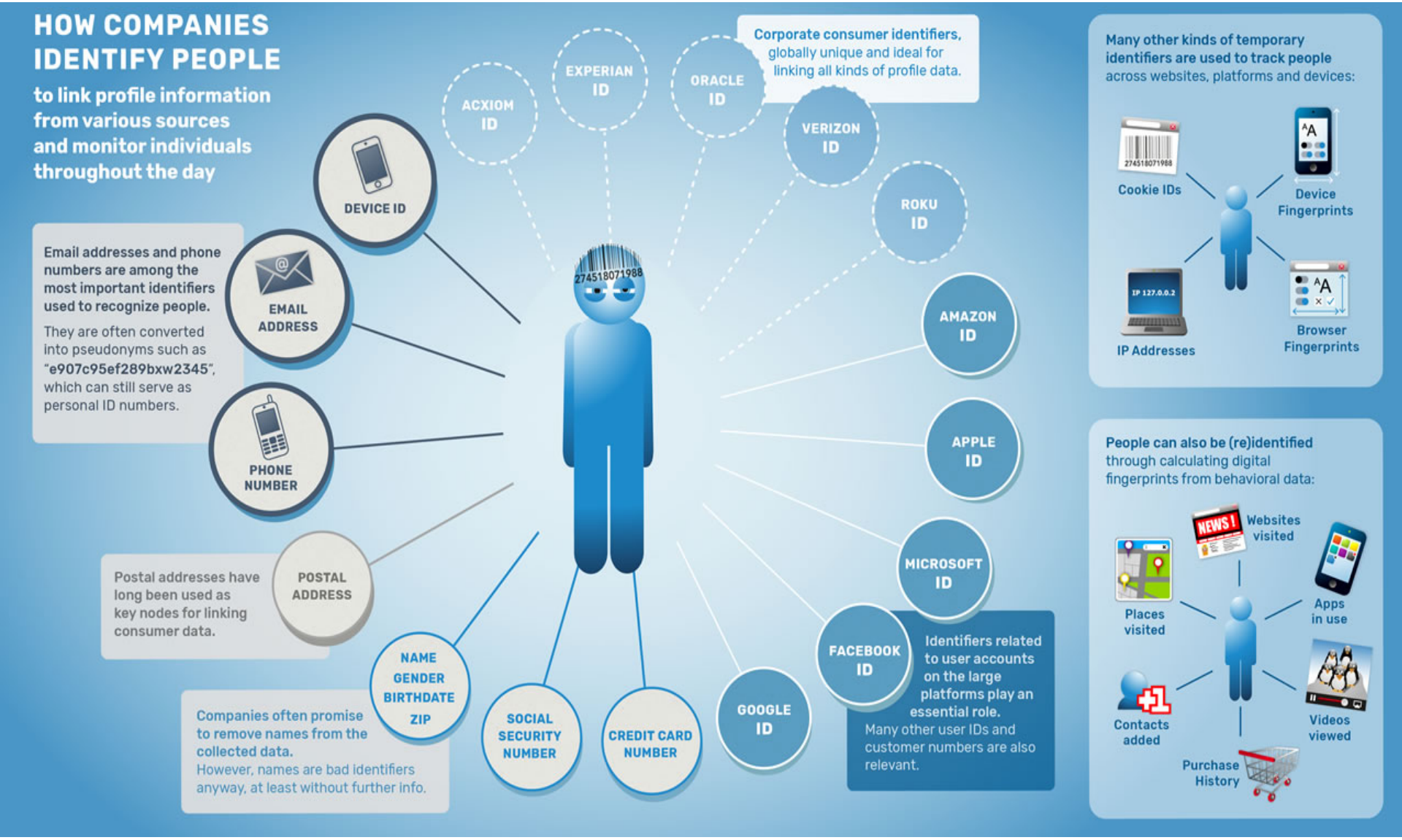
- **Identified**: person who is known, or distinguished from the others in a group
- **Identifiable**: person who is not identified yet, but identification is possible
- **Directly**: reference to a name, in combination with additional information, if the name is not unique

  eg. johnsmith@example.com, "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
ACXIOM ID
EXPERIAN ID
ORACLE ID
Corporate consumer identifiers, globally unique and ideal for linking all kinds of profile data.
VERIZON ID
ROKU ID
DEVICE ID
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.
EMAIL ADDRESS
PHONE NUMBER
274518071988
AMAZON ID
APPLE ID
MICROSOFT ID
FACEBOOK ID
GOOGLE ID
Identifiers related to user accounts on the large platforms play an essential role.
Many other user IDs and customer numbers are also relevant.
Postal addresses have long been used as key nodes for linking consumer data.
POSTAL ADDRESS
NAME
GENDER
BIRTHDATE
ZIP
SOCIAL SECURITY NUMBER
CREDIT CARD NUMBER
Companies often promise to remove names from the collected data.
However, names are bad identifiers anyway, at least without further info.
Many other kinds of temporary identifiers are used to track people across websites, platforms and devices:
Cookie IDs
Device Fingerprints
IP Addresses
Browser Fingerprints
People can also be (re)identified through calculating digital fingerprints from behavioral data:
Websites visited
Places visited
Apps in use
Contacts added
Videos viewed
Purchase History

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 on 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

GDPR

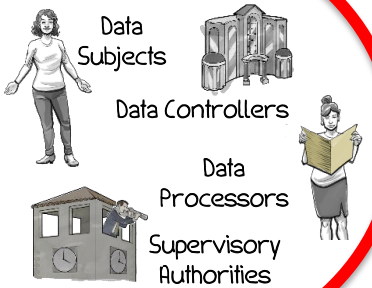
TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations

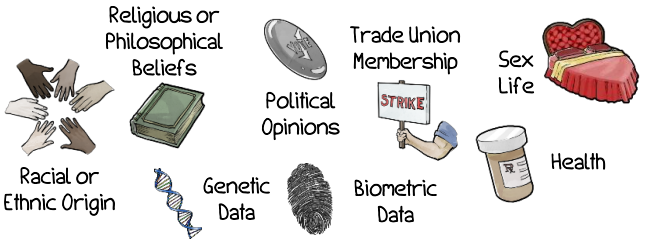
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS



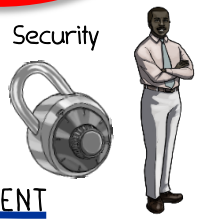
PERSONAL DATA

SENSITIVE DATA



RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security



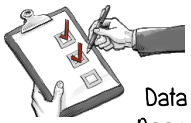
Data Protection Officer (DPO)

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.

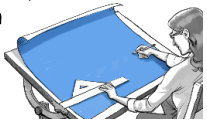
Data Impact Assessment



For high risk situations

Data Protection by Design

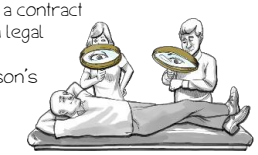
built in starting at the beginning of the design process



LAWFUL PROCESSING

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

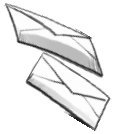
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

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

DATA BREACH NOTIFICATION

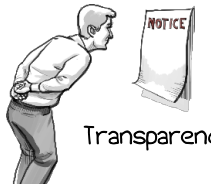


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making

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

Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

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

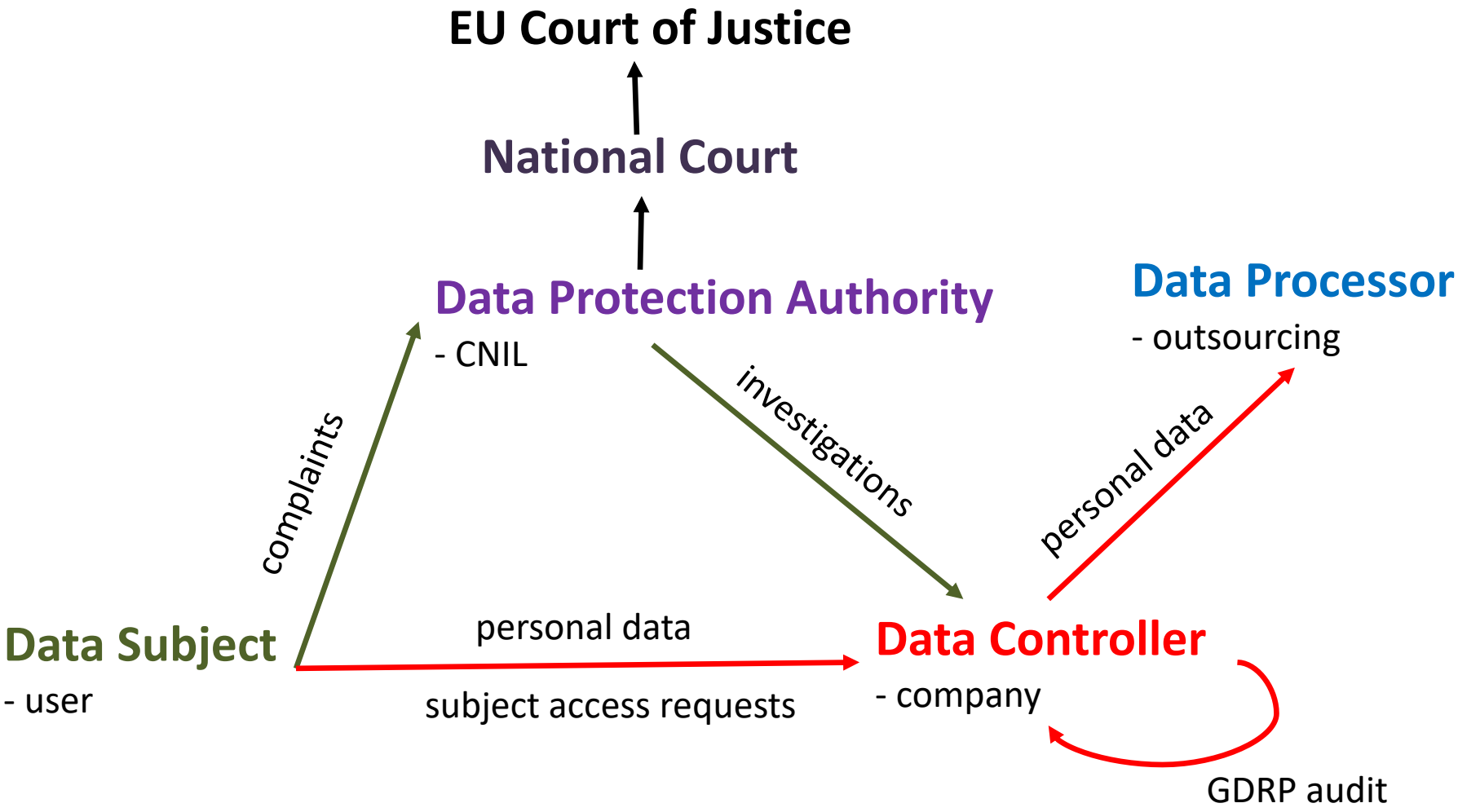
MAJOR ENTITIES

Slides of Cristiana Santos

GDPR major entities

- **Data Subject**
  - us, users
- **Data Controller**
  - company/entity with whom the data subject interacts with
- **Data Processor**
  - processes personal data of the data subject on behalf of the data controller
    - e.g. A company MyBox puts user's data on Google Drive. MyBox is a data controller, while Google is a data processor.

GDPR major entities



New role inside a company

- **Data Protection Authority**
  - legal supervisory authority that investigates complaints and makes decisions

- Each data controller (company) needs to have a **Data Protection Officer (DPO)** who
  - ensures legal compliance with GDPR at the corporate level
  - deals with subject access requests (SAR)

GDPR

TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations

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

THE PLAYERS

Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

PERSONAL DATA

Identified

Identifiable

SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Sex Life

Genetic Data

Biometric Data

Health

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

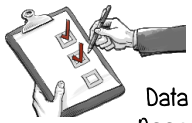
Security

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.

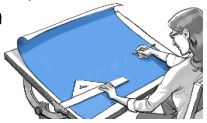


Data Impact Assessment

For high risk situations

Data Protection by Design

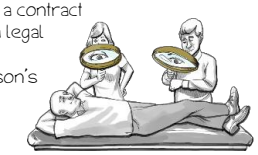
built in starting at the beginning of the design process



LAWFUL PROCESSING

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

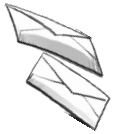
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

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

DATA BREACH NOTIFICATION

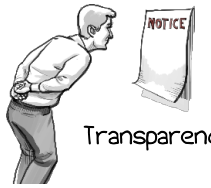


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making

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

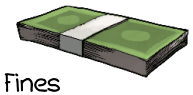
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

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

TEACHPRIVACY

2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

TERRITORIAL SCOPE

Slides of Cristiana Santos

Territorial Scope of GDPR (Art. 3)

GDPR applies to …

- Data controllers and data processors **in the EU**
  →(location of the company)

- Processing of **personal data of data subjects in the EU** (even though the controllers or processors are not in the EU) when
  - offering goods or services irrespectively whether free or paid
  - monitoring their behavior as far as their behavior takes place within the EU

  →(location of the user)

Exercises: does GDPR cover the following cases?

Sara, a Moroccan MSc student, is visiting facebook.com during her lunch break at SKEMA (France). Sara is submitting to facebook.com her personal data, such as pictures and messages. Does GDPR apply to the data of Sara and why?

Exercises: does GDPR cover the following cases?

A French citizen Carine enters the office of Apple in the New York city and is presenting her ID card at the entrance. Apple registers the ID card in their system. Does GDPR apply to the personal data (ID card) of Carine and why?

Exercises: does GDPR cover the following cases?

John is in Australia and is visiting the website of lemonde.fr. Upon the visit, he provides his unique identifier stored in the browser cookie to lemonde.fr. Does GDPR apply to John's personal data (his browser identifier) and why?

GDPR

TERRITORIAL SCOPE

EU Establishments

Non-EU Established Organizations
Offer goods or services or engaging in monitoring within the EU.

THE PLAYERS

Data Subjects

Data Controllers

Data Processors

Supervisory Authorities

PERSONAL DATA

Identified

Identifiable

SENSITIVE DATA

Racial or Ethnic Origin

Religious or Philosophical Beliefs

Political Opinions

Trade Union Membership

Genetic Data

Biometric Data

Health

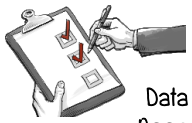
Sex Life

RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

Security

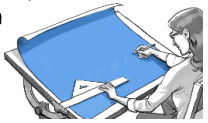
Data Protection Officer (DPO)
Designate DPO if core activity involves regular monitoring or processing large quantities of personal data..

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

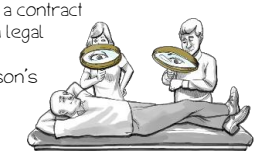
Data Protection by Design
built in starting at the beginning of the design process



LAWFUL PROCESSING

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

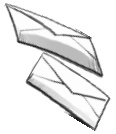
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



CONSENT

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

DATA BREACH NOTIFICATION

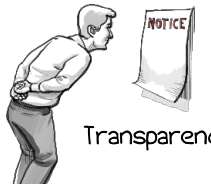


A *personal data breach* is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

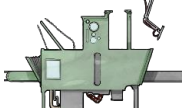
Notify supervisory authorities no later than 72 hours after discovery.

RIGHTS OF DATA SUBJECTS



Transparency

Automated Decision Making



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

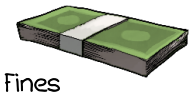
Right to Erasure

Access and Rectification

Purpose Specification and Minimization

Right to Data Portability

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)

INTERNATIONAL DATA TRANSFER

Adequate Level of Data Protection

Privacy Shield

Model Contractual Clauses

TEACHPRIVACY 2019

www.teachprivacy.com

Workforce awareness training by Prof. Daniel J. Solove

ENFORCEMENT

Slides of Cristiana Santos

GDPR Fines

- Companies that collect personal data are should be compliant with GDPR
- **Fines**: **20M euro or 4% global annual turnover** (whatever is bigger) **per violation**!

A startup MyBooks consists of two people and does not have a Data Protection Officer (DPO). MyBooks collects users' names, surnames, dates of birth and email addresses. The startup violates the consent requirements of GDPR because MyBooks gives access to the users' data to third party advertising services. DPA detects violations, tries to reach out to MyBooks but never gets any response. DPA fines MyBooks 5M euros. MyBooks is a bankrupt now.

The CNIL First GDPR Fine!

CNIL.

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC

21 January 2019

On 21 January 2019, the CNIL's restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.