

# 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

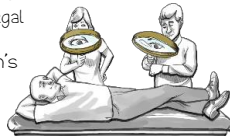
Non-EU Established Organizations

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

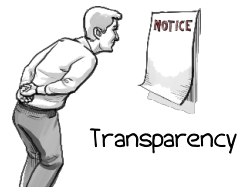
## LAWFUL PROCESSING

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

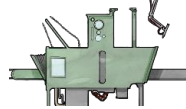


## RIGHTS OF DATA SUBJECTS



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

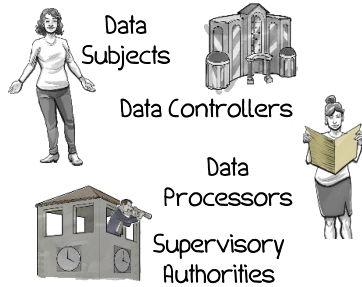


Purpose Specification and Minimization



Right to Data Portability

## THE PLAYERS

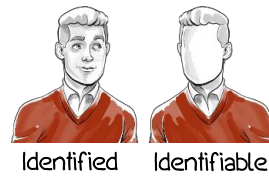


EU Establishments

Non-EU Established Organizations

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

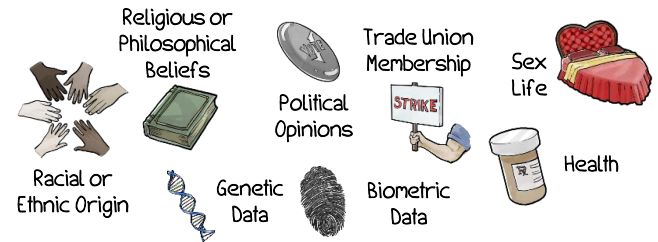
## PERSONAL DATA



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



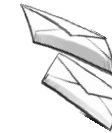
## CONSENT



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

# GDPR

## DATA BREACH NOTIFICATION

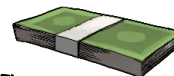


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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

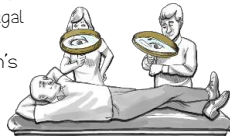
Non-EU Established Organizations

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

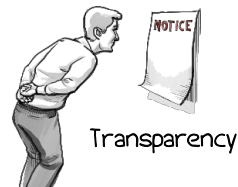
## LAWFUL PROCESSING

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

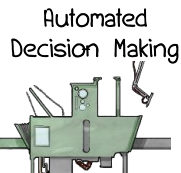
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



## RIGHTS OF DATA SUBJECTS



Transparency



Automated Decision Making

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

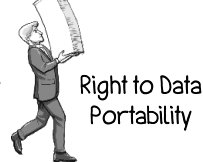


Access and Rectification



Purpose Specification and Minimization

Right to Erasure



Right to Data Portability

## CONSENT



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

## 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

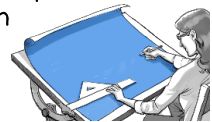
Maintain a documented register of all activities involving processing of EU personal data.



Data Impact Assessment

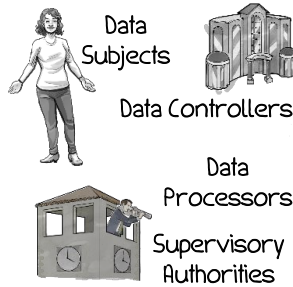
For high risk situations

Data Protection by Design

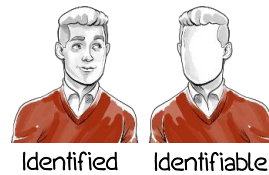


built in starting at the beginning of the design process

## THE PLAYERS



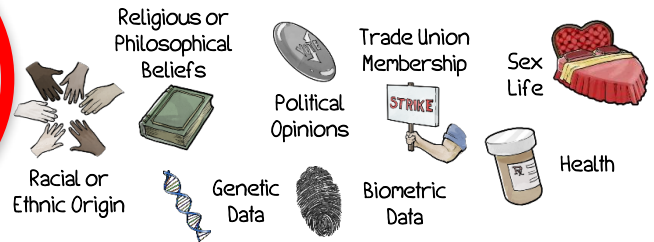
## PERSONAL DATA



Identified

Identifiable

## SENSITIVE DATA



## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

# GDPR

## DATA BREACH NOTIFICATION

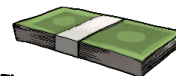


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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)



Privacy Shield



Model Contractual Clauses

## INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection



# 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

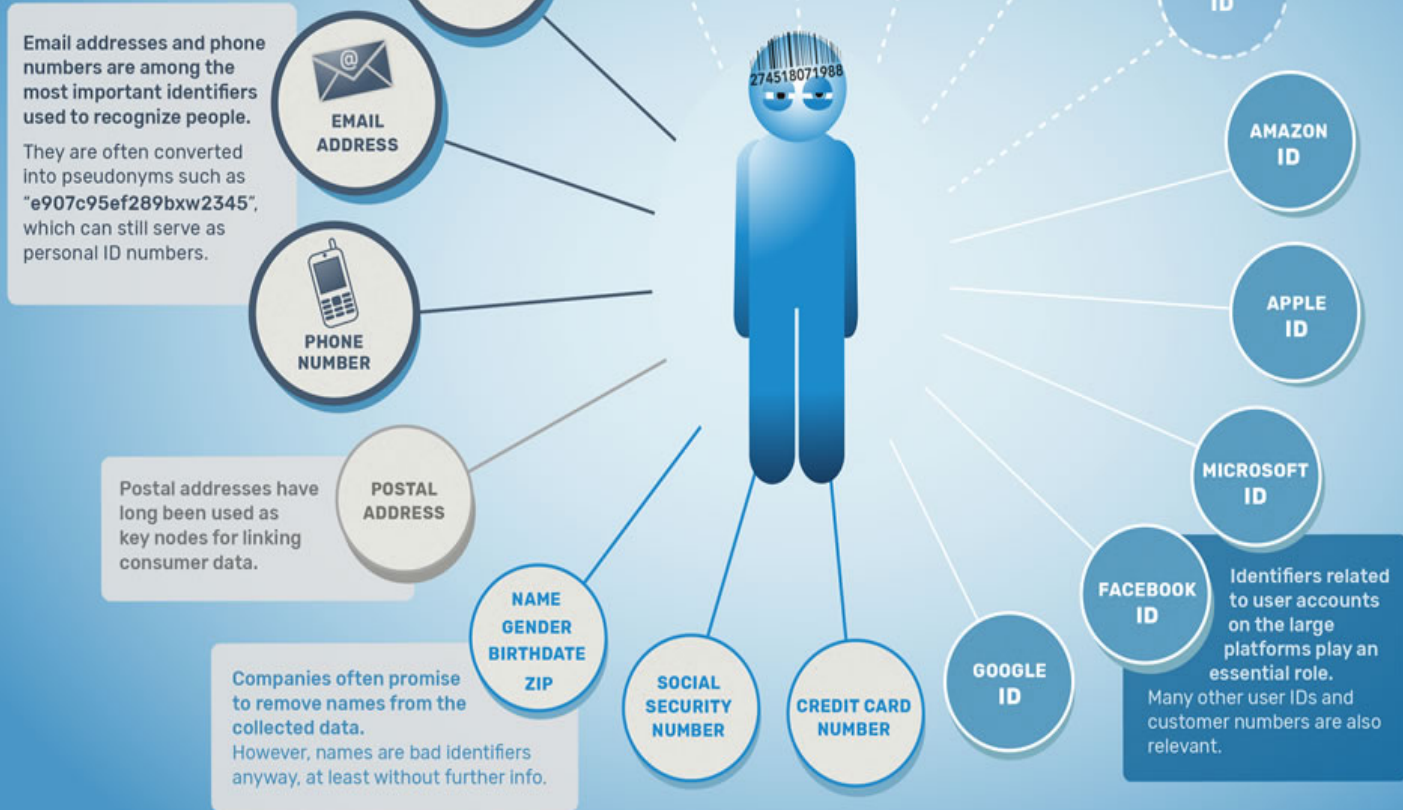
- **Identified:** person who is known, or distinguished from the others in a group
- **Identifiable:** person who is not identified yet, but identification is possible
- **Directly:** reference to a name, in combination with additional information, if the name is not unique  
eg. [johnsmith@example.com](mailto:johnsmith@example.com), “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





## 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



## TERRITORIAL SCOPE

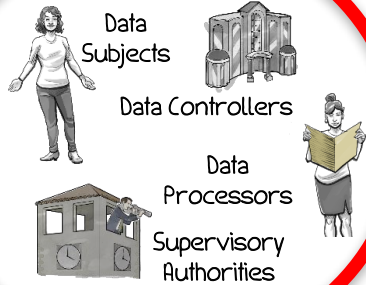


EU Establishments

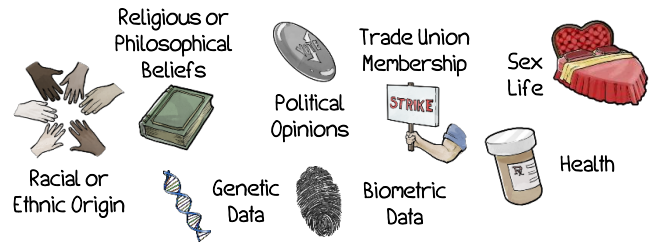
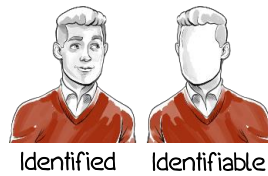
Non-EU Established Organizations

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

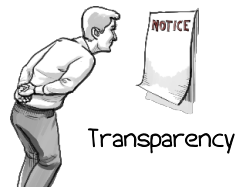


## CONSENT



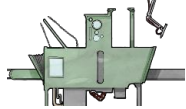
Consent must be freely given, specific, informed, and unambiguous.

## 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

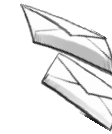
Data Protection by Design

built in starting at the beginning of the design process



# GDPR

## DATA BREACH NOTIFICATION

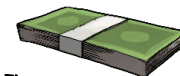


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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



# GDPR major entities

17

- **Data Subject**
  - us, users

## 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/>

# GDPR major entities

19

- **Data Subject**
  - us, users
- **Data Controller**
  - company/entity with whom the data subject interacts with

---

## Art. 4 GDPR

# Definitions

‘**controller**’ means 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;

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

# GDPR major entities

21

- **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.

---

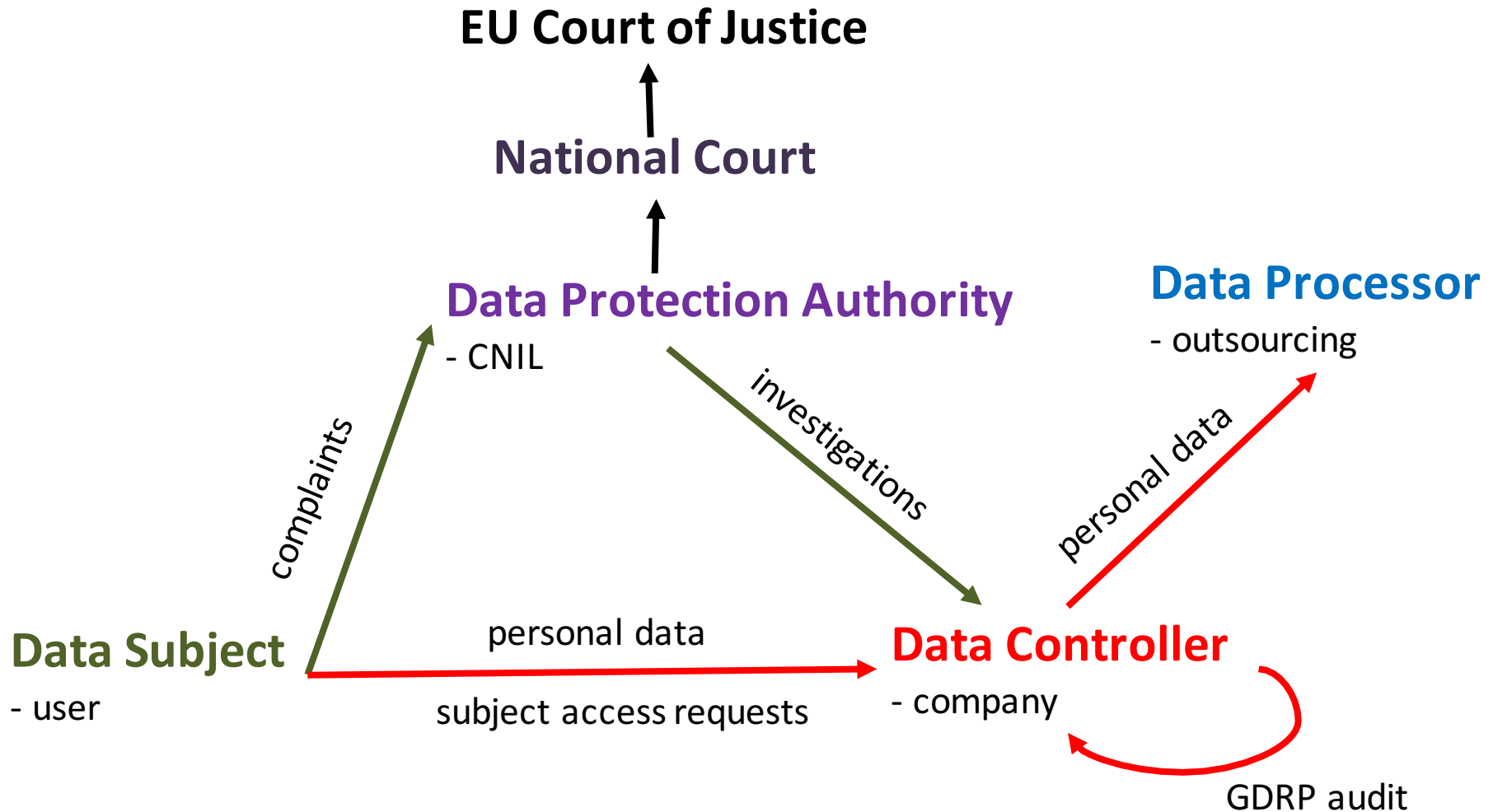
## Art. 4 GDPR

# Definitions

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**;

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

# GDPR major entities



# Who takes care of legal compliance?

24

- **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)



## TERRITORIAL SCOPE

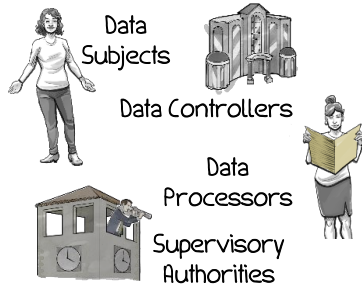


EU Establishments

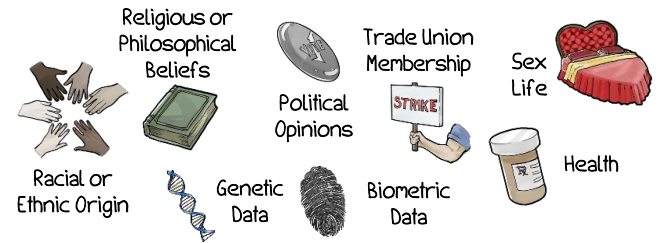
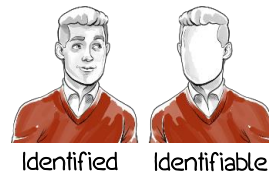
Non-EU Established Organizations

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

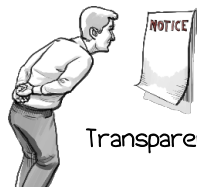


## CONSENT



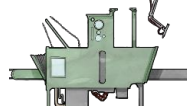
Consent must be freely given, specific, informed, and unambiguous.

## 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

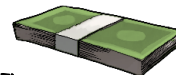


Right to Data Portability



# GDPR

## 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)

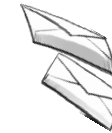


Privacy Shield



Model Contractual Clauses

## 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.

## INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection

# 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.*

## TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations

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

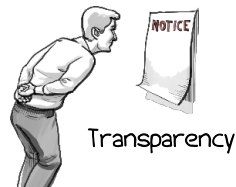
## LAWFUL PROCESSING

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

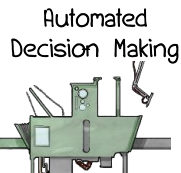
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



## RIGHTS OF DATA SUBJECTS



Transparency



Automated Decision Making



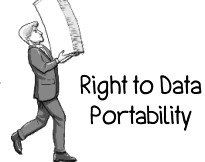
Right to Erasure



Access and Rectification



Purpose Specification and Minimization



Right to Data Portability

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

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

## CONSENT



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

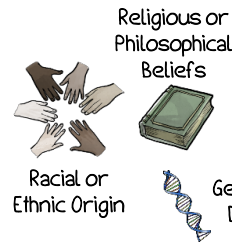


## PERSONAL DATA



Identified

Identifiable



Religious or Philosophical Beliefs

Racial or Ethnic Origin



Genetic Data



Political Opinions



Trade Union Membership

Biometric Data

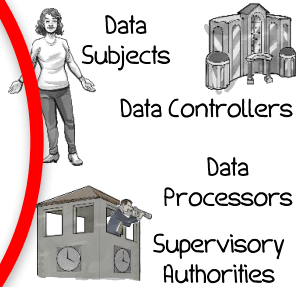


Sex Life



Health

## THE PLAYERS



Data Subjects



Data Controllers



Data Processors

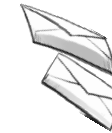


Supervisory Authorities

## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

# GDPR

## DATA BREACH NOTIFICATION

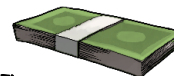


A personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

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



# TERRITORIAL SCOPE

# 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?

## TERRITORIAL SCOPE



EU Establishments

Non-EU Established Organizations

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

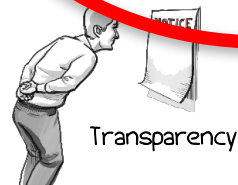
## LAWFUL PROCESSING

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

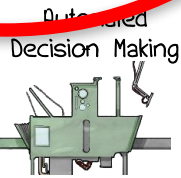
- performance of a contract
- compliance with a legal obligation
- to protect a person's vital interests
- task in the public interest
- legitimate interests



## RIGHTS OF DATA SUBJECTS



Transparency



Automated Decision Making



Right to Erasure



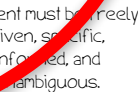
Access and Rectification



Purpose Specification and Minimization



Right to Data Portability



## CONSENT

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



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

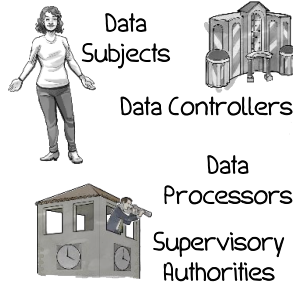
Data Protection by Design

built in starting at the beginning of the design process

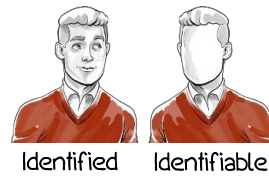


## RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS

## THE PLAYERS



## PERSONAL DATA

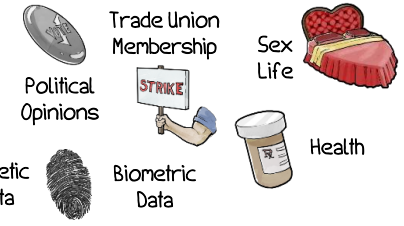


Identified Identifiable



Religious or Philosophical Beliefs  
Racial or Ethnic Origin  
Genetic Data

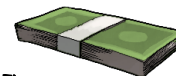
## SENSITIVE DATA



Trade Union Membership  
Sex Life  
Health  
Biometric Data

# GDPR

## 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)



Privacy Shield



Model Contractual Clauses

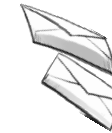
## INTERNATIONAL DATA TRANSFER



Adequate Level of Data Protection

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

Notify supervisory authorities no later than 72 hours after discovery.



## 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."



# LAWFUL PROCESSING OF PERSONAL DATA

# Legal bases for processing personal data

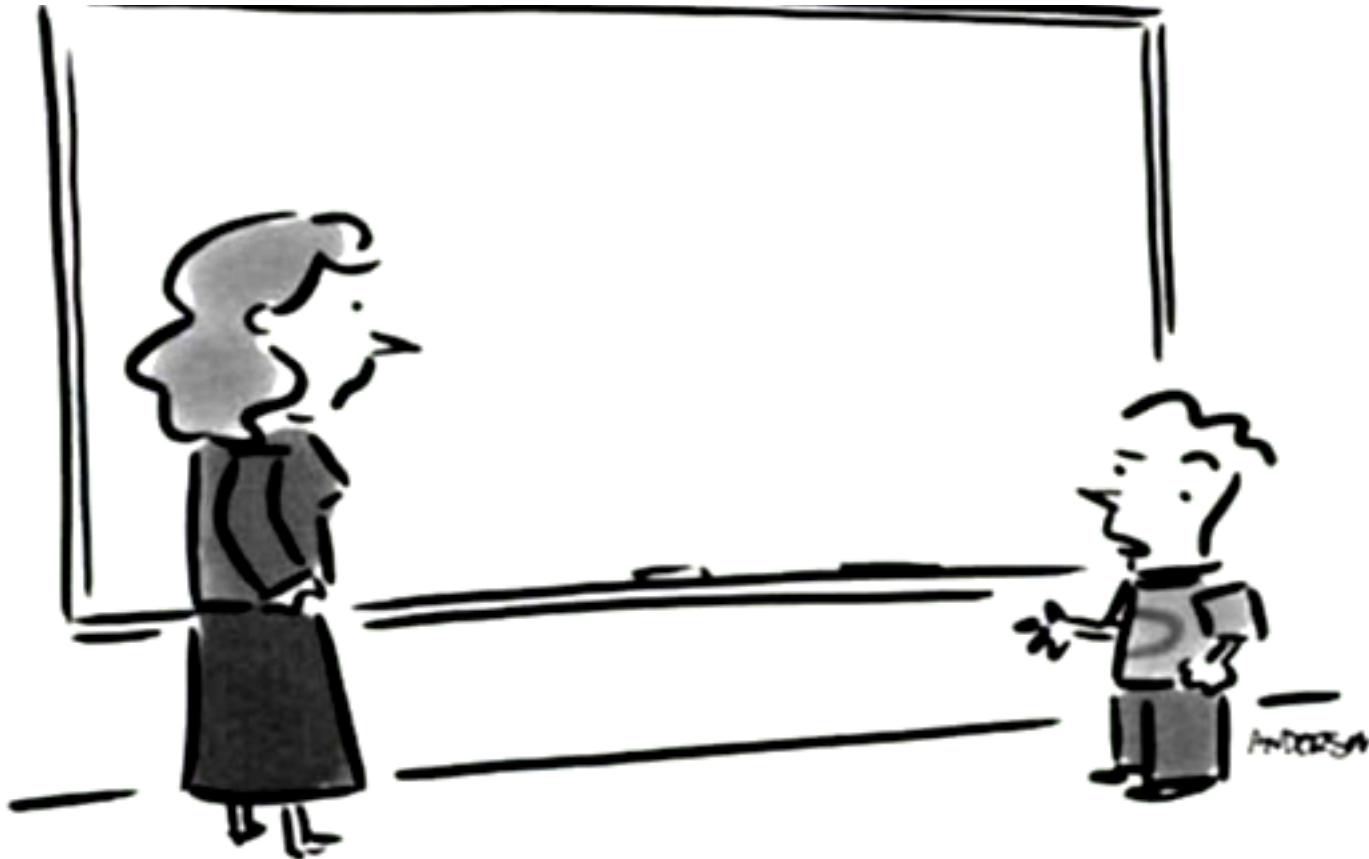
6º, §40



- 1. Consent**
- 2. Contract necessity** for the performance of a contract between the controller and subject
- 3. Compliance with a Legal Obligation**
- 4. Task in the Public Interest**, official functions or a task in the public interest
- 5. Protecting Vital Interests** of the data subject, eg. to protect someone's life during medical emergency (life and death)
- 6. Legitimate Interest of the data controller** balanced against the rights and freedoms of the individual



# Consent



“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”



# Consent

- **What?** Mechanism to give data subjects control/**choice** over whether or not personal data concerning them will be processed
- **When?** Given before processing, 6<sup>o</sup> “has given” (29WP 257)
- **How?** No limits on form
- **Elements of valid consent** 4(11)
  1. Free
  2. Specific
  3. Informed
  4. Unambiguous
  5. Explicit



“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”

# 1. Freely given Consent

- Not valid when there is no real choice:
  - i. **Imbalance of power**: data subject is compelled, pressured, influenced, fear to consent
  - ii. **Conditionality**: consent asked in the scope of a contract or service
  - iii. **Granularity**: give a separate consent from other matters
  - iv. **Detriment**: has to endure negative consequences by not consenting



## i. Free vs Imbalance of Power

- §43 Presumption of **imbalance of power** if controller is **public authority, employer, medical service** (dominant position). Data subject fearing adverse consequences, has **no** realistic alternative to accept the processing terms (invalid consent)
- **Other lawful bases** more appropriate to the activity of public authorities (legal obligation, public interest)
- Cases:
  - Fear or real risk of detrimental effects as a result of a refusal
  - Risk of deception, intimidation, coercion or significant negative consequences, e.g. substantial extra costs for non consenting
  - Compulsion, pressure or inability to exercise free will



A local municipality is planning road maintenance works. The municipality offers its citizens the opportunity to subscribe to an email list to receive updates on the progress of the works and on expected delays.

The municipality makes clear that there is **no obligation to participate** and asks for consent to use email addresses for this (exclusive) purpose. Citizens that do not consent will not miss out on **any core service** of the municipality or the exercise of any right, so they are able to give or refuse their consent to this use of data freely. All information on the road works will also be available on the municipality's website.



## ii. Free vs Conditionality

- 7(4), §43: **tying, bundling, disguising** the consent request as a **condition** for the performance of contract. Consent and contract cannot be merged
- **Assessment:**
  - Scope/**core** of contract; data necessary for that contract
  - “**Necessity**” to fulfill the contract with each individual data subject, eg. address for goods to be delivered, credit card details for payment
  - Direct/objective **link** between the processing of the data and the purpose of the execution of the contract



## ii. Free vs Conditionality

Association of car drivers offers the possibility for members to get a replacement vehicle in the scope of breakdown assistance, only if drivers consent with the tracking of their data and monitoring of their driving behavior via telematics

Bank asks customers for consent to allow third parties to use their payment details for direct marketing purposes. The customer's refusal to consent implies denial of banking services, closure of the bank account, or an increase of fees

## iii. Free vs Granularity

- § 43 § 32: **Separate consent** per each purpose; separation of different purposes, operation, T&Cs, *1:1*

### Is it granular?

Within the same consent request a retailer asks its customers for consent to use their data to send them **marketing by email**, and also, to **share their details with other companies** within their group.

## iv. Free vs Detriment

- §42: Withdraw consent without detriment
  - eg. not lead to any costs, no clear disadvantage for those withdrawing consent: deception, intimidation, coercion, downgrading of the service, or significant negative consequence

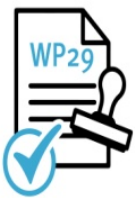
When downloading a lifestyle mobile app, the app asks for consent to access the phone's accelerometer. When the user revokes consent, the app now only works to a limited extent.

Celine subscribes to a fashion retailer's newsletter with general discounts. The retailer asks for consent to collect more data on shopping preferences to tailor the offers based on shopping history, or a questionnaire that is voluntary to fill out. When she revokes consent, she will receive non-personalized fashion discounts again.



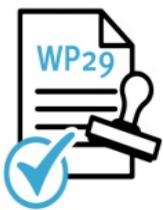
## 2. Specific Consent

- 6(1)(a), § 43, § 32, 29WP 03/2013: **consent specific per purpose**
- **Criteria:**
  - **Purpose specification:** as a safeguard to avoid “function creep” or widening or blurring of purposes; explain what and why
  - **Granularity in consent requests:** separate opt-in for each purpose
  - **Clear separation of information** on obtaining consent for data processing activities, from information about other matters
- Eg. general purposes:
  - “improving users' experience”, “marketing purposes”, “IT-security purposes”, “future research”



## 2. Specific Consent

A cable TV network **collects subscribers' personal data**, based on their consent, to present them with personal suggestions for new movies they might be interested in based on their viewing habits. After a while, the TV network **decides to enable third parties to send** (or display) targeted advertising on the basis of the subscriber's viewing habits.



# 3. Informed Consent





29WP 259 Guidelines on Consent

- **What are minimum content requirements (transparency)?**
  - § 42: Identity of the (joint) controller
  - § 42: purposes of the processing
  - Type of data to be collected
  - 7(3) existence of the right to withdraw consent
  - 22 (2)(c): Info on the use of data for automated decision-making
  - 46: Info on the risks of data transfers
- **How to provide information? 7(2), § 32, § 42**
  - Free form/shape, eg. written or oral statements, or audio or video messages
  - Clear and plain language for lay people - understandable
  - Distinguishable (separate and distinct) from other matters
  - Should not contain unfair terms, Directive 93/13/EC – if doubt, pro consumer
  - Intelligible and easy accessible form – not hidden in T&Cs
  - WP on Transparency: precise and complete (layered info)



# 4. Unambiguous Consent



	<b>GDPR</b> 4(11) §3	<b>29WP</b> 259 on Consent
<p><b>Valid</b></p> 	<ul style="list-style-type: none"> <li>• any oral/written statement, or clear affirmative action</li> <li>•ticking a box when visiting a website</li> <li>•choosing technical settings for information society services</li> </ul>	<p>“if you – click a button or link, tick a box, swipe a bar on a screen, waive in front of a smart camera, turn a smartphone around clockwise, – you agree to the use of information X for purpose Y”</p>
<p><b>Non Valid</b></p> 	<ul style="list-style-type: none"> <li>•Inaction, silence, inferred</li> <li>•pre-ticked boxes</li> <li>•condition to other actions</li> </ul>	<ul style="list-style-type: none"> <li>•scrolling down a website</li> <li>• swiping through a website (difficult to distinguish)</li> </ul>



# 5. Explicit Consent

- **When?**
  - 9<sup>o</sup> processing sensitive data: healthcare data; 49<sup>o</sup> data transfers to 3rd countries; 22<sup>o</sup> automated individual decision-making, including profiling
- **How?**
  - eg. filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature

An airline company, Holiday Airways, offers an assisted travelling service for passengers that cannot travel unassisted, for example due to disability. Holiday Airways requires customers to provide information on the health condition to be able to arrange the appropriate services (e.g. wheelchair on the arrival gate, or an assistant travelling from A to B.) Holiday Airways asks for explicit consent to process the health data of this customer for the purpose of arranging the requested travel assistance. Moreover, flights to Budapest remain available without travel assistance.



# Obligation to Demonstrate Consent?



- 7(1), §42
- Controller has the burden of proof
- **How to demonstrate?**
  - **Record** of consent statement received: who, what, when, how  
Eg. name, session Id, username, dated doc, documentation of the consent workflow at the time of the session, online timestamp, copy of the info presented, form
- **Expiration date?**
  - No “evolving consent” vs specific
  - Depends on context, scope of original consent, expectations of the data subject, evolution of processing.
  - **Refreshed** consent at appropriate intervals





# Withdrawal of Consent 7(3), 17(1)b, §39



- **When?** Be informed before, at any time
- **How?** As easy as to give, without undue effort e.g. mouse-click, swipe, keystroke, website/app, log-on account, interface of an IoT device, e-mail
- **Without detriment** – free or without lowering service levels
- Changes to the legal basis must be **notified to a data subject** - 13<sup>o</sup>, 14<sup>o</sup>, principle of transparency
- Stop processing! **Exceptions:**
  - 17(3) for legal obligation, legal claim
  - 15(1)(e) storage kept for archiving for the public interest, scientific, historical research, statistical purposes
  - 6 (1) other legal basis

# Withdrawal of Consent

When the data subject withdraws her consent, but the controller wants to continue processing personal data on another legal basis, can they silently swap from consent to other basis?

A music festival sells tickets through an online ticket agent. With each online sale, consent is requested in order to use contact details for marketing purposes and customers can select either No or Yes. The controller informs customers that they have the possibility to withdraw consent by contacting a call centre on business days between 8am and 5pm, free of charge.

## TERRITORIAL SCOPE

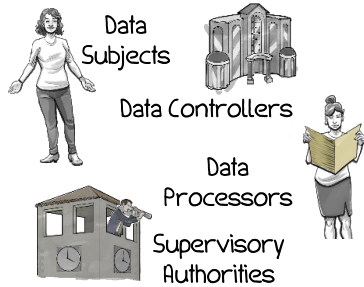


EU Establishments

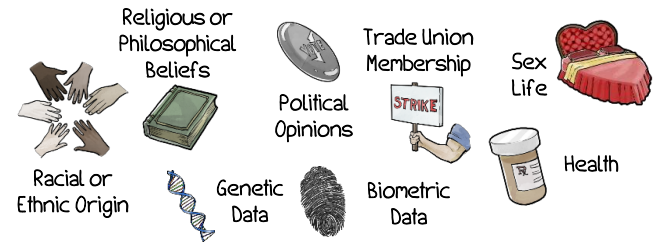
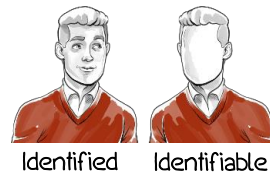
Non-EU Established Organizations

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

## THE PLAYERS



## PERSONAL DATA

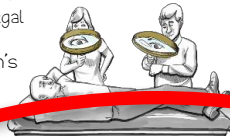


## SENSITIVE DATA

## 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

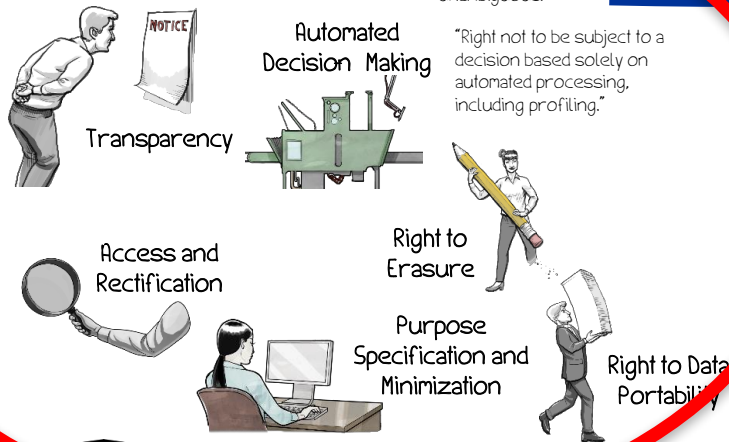


## CONSENT



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

## RIGHTS OF DATA SUBJECTS



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

Right to Data Portability



Right to Erasure

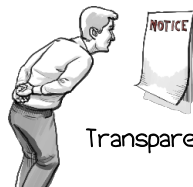
Purpose Specification and Minimization



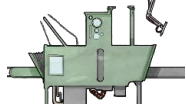
Access and Rectification



Transparency



Automated Decision Making



## 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)

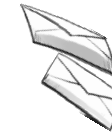


Privacy Shield



Model Contractual Clauses

## 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.

## INTERNATIONAL DATA TRANSFER

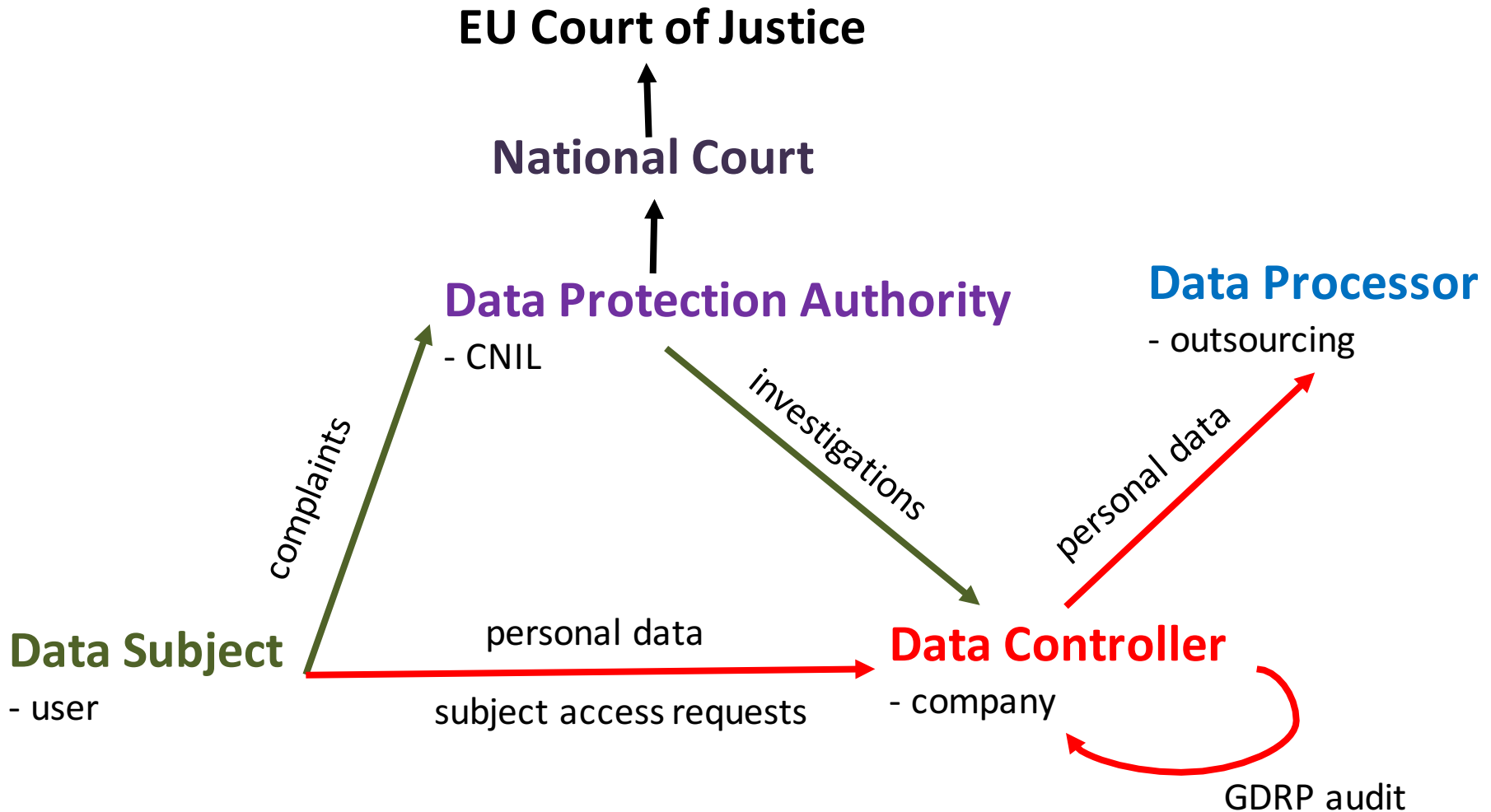


Adequate Level of Data Protection



# RIGHTS OF DATA SUBJECTS

# GDPR major entities





## Chapter 3

# Rights of the data subject

5

**To implement these rights, a data controller must authenticate data subjects first!**

**Section 1 – Transparency and modalities**

Article 12 – Transparent information, communication and modalities for the exercise of the rights of the data subject

**Section 2 – Information and access to personal data**

Article 13 – Information to be provided where personal data are collected from the data subject

Article 14 – Information to be provided where personal data have not been obtained from the data subject

Article 15 – Right of access by the data subject

**Section 3 – Rectification and erasure**

Article 16 – Right to rectification

Article 17 – Right to erasure ('right to be forgotten')

# Data Subject rights vs Data Controller fears

58

Data Subject



- How do I exercise my rights?
- How do I prove my identity to the controller?
- Can they **impersonate** me? (use my credentials to get my data)
- Will they do **abusive identity check**? (ask me for more than need)

Data Controller



- Is the request legitimate?
- What is necessary to identify the subject's data?
- What if the data subject is illegitimate?
- What if I release the data of Alice to Bob?

**More details on the next lectures...**