UNIVERSITÉ
CÔTE D'AZUR

General Data Protection Regulation

Cristiana Santos

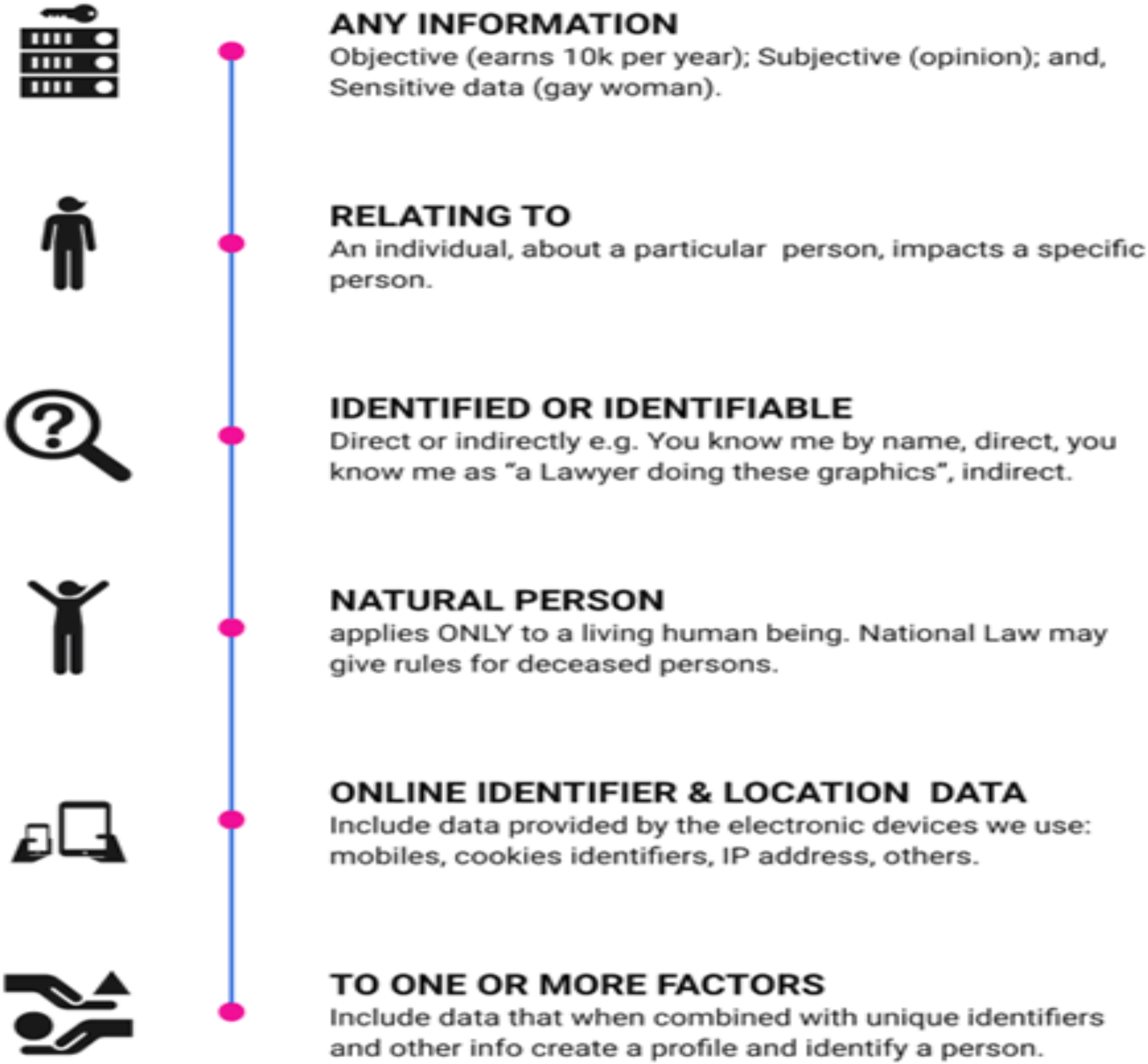
February 27th, 2019

Security and ethical aspects of data

Université Cote d'Azur

Content Overview

I. GDPR
   1. What is personal data
   2. Legal basis for processing
      - Consent



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, 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

2. 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

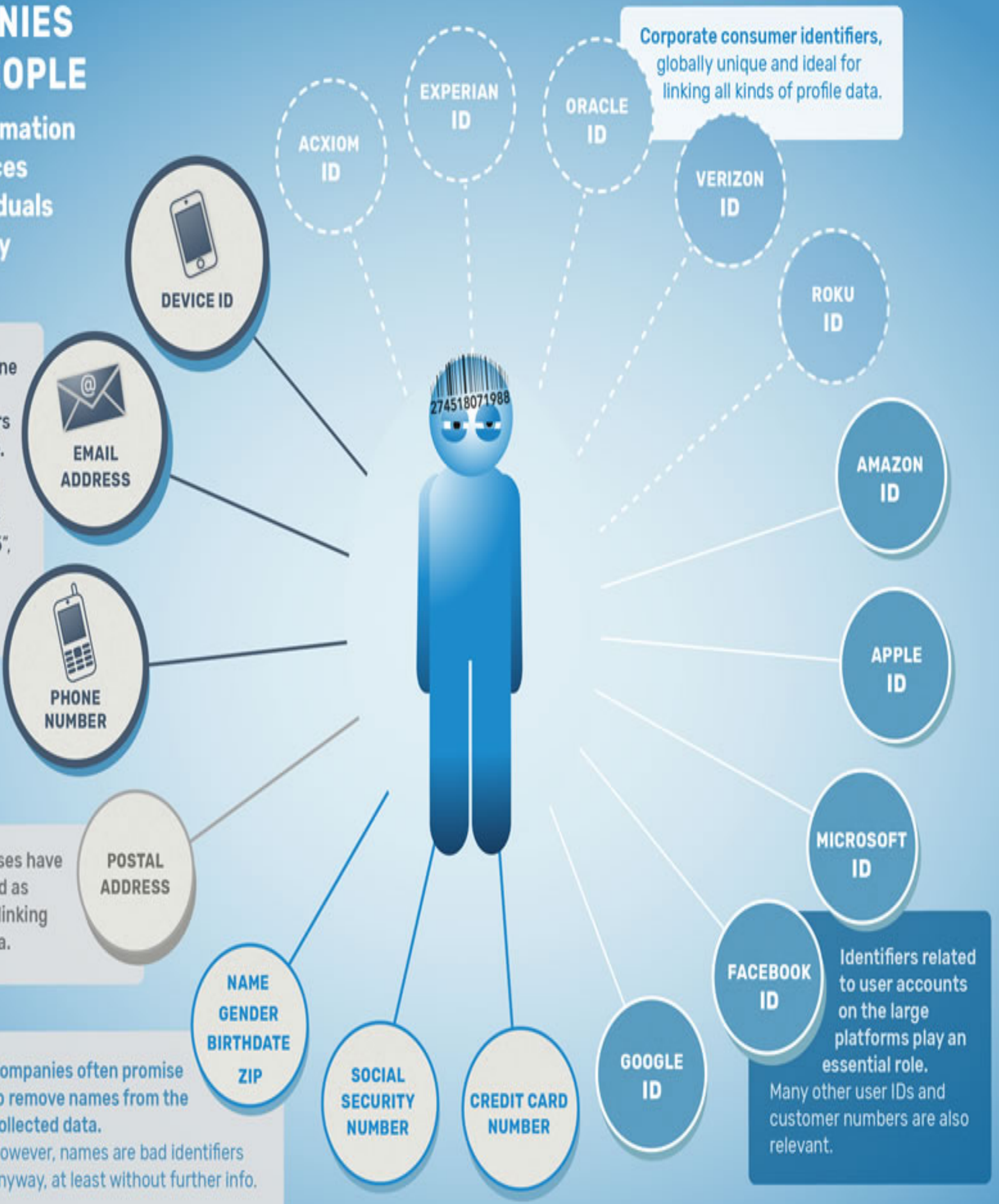
  eg. johnsmith@example.com, "elderly man lives at nr 15 Purple St and drives a Porsche", "Maria's foster mum, from Year 4 at Junior School"
- **Indirectly:** unique combinations of indirect identifiers that allow a person to be singled out from others

  eg. car registration number, combination of significant criteria (age, occupation, place of residence)

Direct Identifiers	Online Identifiers	Indirect Identifiers
Name	IP address	Physical
Address details	Cookies	Physiological
Email address	RFID Tags	Genetic
ID number	MAC addresses	Mental
Location data	Advertising IDs	Economic
	Pixel tags	Cultural
	Account usernames	Social Identity
	Device fingerprints	

HOW COMPANIES IDENTIFY PEOPLE

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



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

Email addresses and phone numbers are among the most important identifiers used to recognize people.

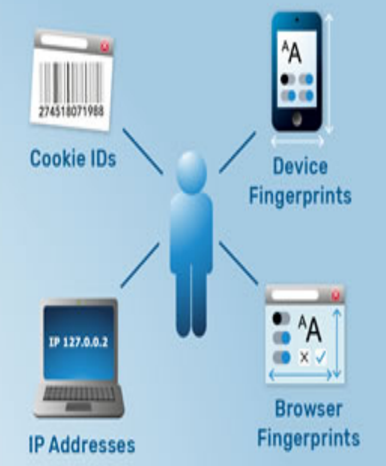
They are often converted into pseudonyms such as "e907c95ef289bxw2345", which can still serve as personal ID numbers.

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

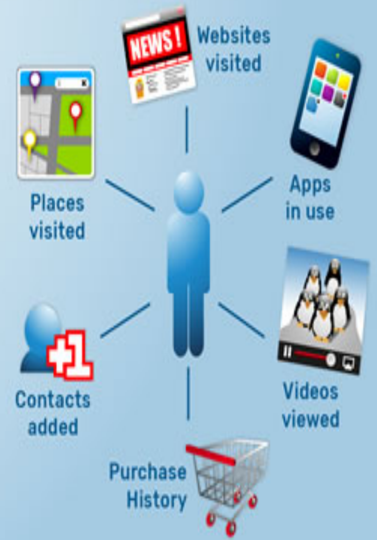
Companies often promise to remove names from the collected data.
However, names are bad identifiers anyway, at least without further info.

Identifiers related to user accounts on the large platforms play an essential role.
Many other user IDs and customer numbers are also relevant.

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 on indirectly

  eg. public registry, reverse directory
- By the controller or 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

- The reasonable likelihood of someone linking any piece of information to another person renders more plausible because combining databases becomes daily practice, permiits to distinguish and allows for the identification of a person (intelligence agencies, ‘smart city’ municipalities, advertising, ML algorithms, etc)

Examples: identified or identifiable

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

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)

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

3. 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

Content Overview

I. GDPR
   1. What is personal data
   2. Legal basis for processing
      - Consent

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

- **Where?**
  - 29WP Opinions
  - Arts. 4(11), 6, 7; § 32, 33, 42, 43
  - Arts. 7, 8 Charter of Fundamental Rights EU
- **What?** Mechanism to give data subjects control/**choice** over whether or not personal data concerning them will be processed
- **When?** Given before processing, 6º “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**: DS 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 maters
  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). DS 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

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.

C 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”

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.

A **mobile app for photo editing** asks its users to have their **GPS localization activated** for the **use** of its services. The app also tells its users it will use the collected data for **behavioural advertising purposes**.

Are geo-localisation or online behavioural advertising necessary for the photo editing service?

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

	GDPR 4(11) §3	**29WP** 259 on Consent
Valid YES PLEASE ☑ NO THANKYOU □	• any oral/written statement, or clear affirmative action •ticking a box when visiting a website •choosing technical settings for information society services	"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"
Non Valid	•Inaction, silence, inferred •pre-ticked boxes •condition to other actions	•scrolling down a website • swiping through a website (difficult to distinguish)

5. Explicit Consent

- **When?**
  - 9º processing sensitive data: healthcare data; 49º data transfers to 3rd countries; 22º 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.

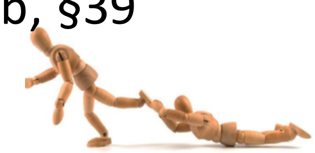
Obligation to Demonstrate Consent?

- 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** - 13º,14º, 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.