Legal

Dr. Balázs Pejó

www.crysys.hu

Agenda

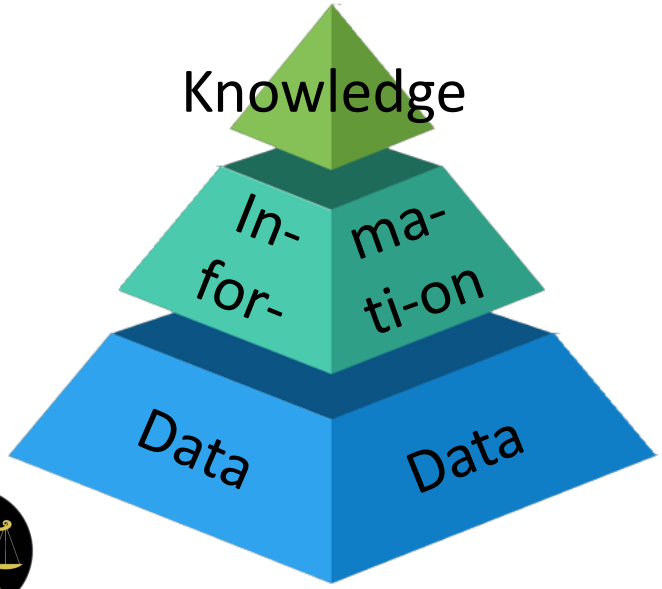
- Dark Patterns
- Tracking
- GDPR
- Deidentification
- Machine Learning
- Anonymization
- Cryptography

- Data Protection / Fundamental Rights
  - US Laws
- Rights of Data Subjects
- Personal / Sensitive / Confidential Data
- Principles of GDPR
  - Lawfulness
  - Consent

- Other EU Laws

Recap

- Dark Patterns (based on Cognitive Biases) nudge customers towards behaving in the company's desired way.
- Profiling can be used for personalized manipulation.
- There are multiple ways one can be tracked on the internet.
- Data is collected by Data Brokers.
- Our data reveals much more about ourself than what we think.



G D P R

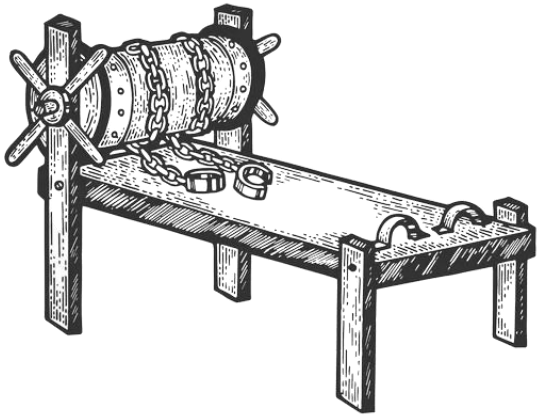
Privacy vs Data Protection

- Data protection is a right to protect any information relating to you as an identified or identifiable natural (living) person.
  - Protection of privacy right with respect to the processing of personal data.
  - Focuses on personal data (both public, non-sensitive and private, sensitive).
  - Has the same meaning in most languages.
  - Not recognized outside EU as a fundamental right.

- Privacy is the right to private and family life, home and communications, to be autonomous, to be let alone.
  - A recognized universal human right in most countries.
  - The interpretation of *privacy* depends on the idiosyncrasies of the language.

Absolute vs Fundamental Right

- Fundamental rights are inherent to all human beings, whatever our nationality, residence, sex, ethnicity, color, religion, language, etc.
- Fundamental rights can be restricted.
  - Freedom can be restricted with jail.
- Absolute rights cannot be restricted.
  - Not to be enslaved, not to be tortured, etc.



- Protection of private life and the protection of personal data are fundamental rights in EU.
  - Everyone has the right to the protection of personal data concerning him or her.

Necessity & Proportionality

- All fundamental rights can be limited following the principle of necessity and proportionality.
- Necessity: restriction of the right is necessary.
  - For social welfare or to exercise another fundamental right.
- Proportionality: the negative effects of this restriction must not outweigh its benefits.
  - Must always be justified.

- They must be considered in relation to its function in society and be balanced against other fundamental rights.
  - It is subject to reasonable restrictions for the protection of general welfare.

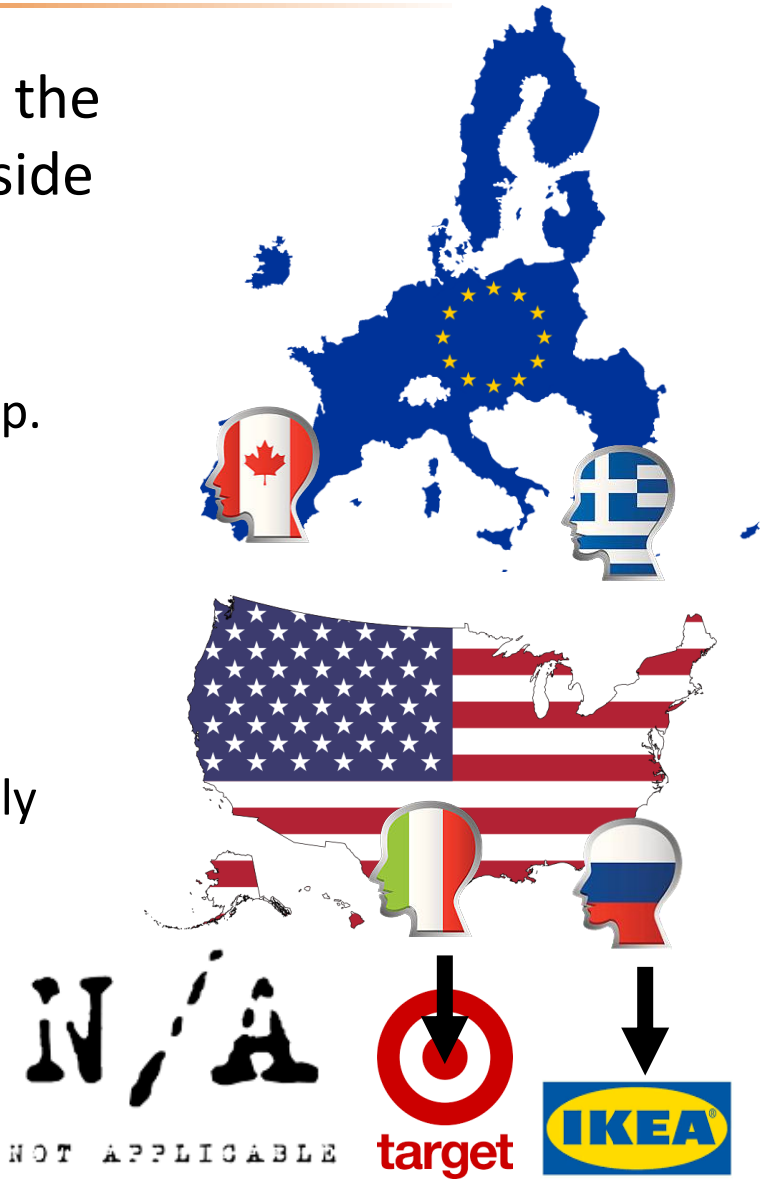
Examples

- Necessity
  - Surveillance
    Right to Data Protection vs
    Right to Liberty and Security

- Proportionality
  - Street View
    It must be considered in relation
    to its function in society.

Coverage

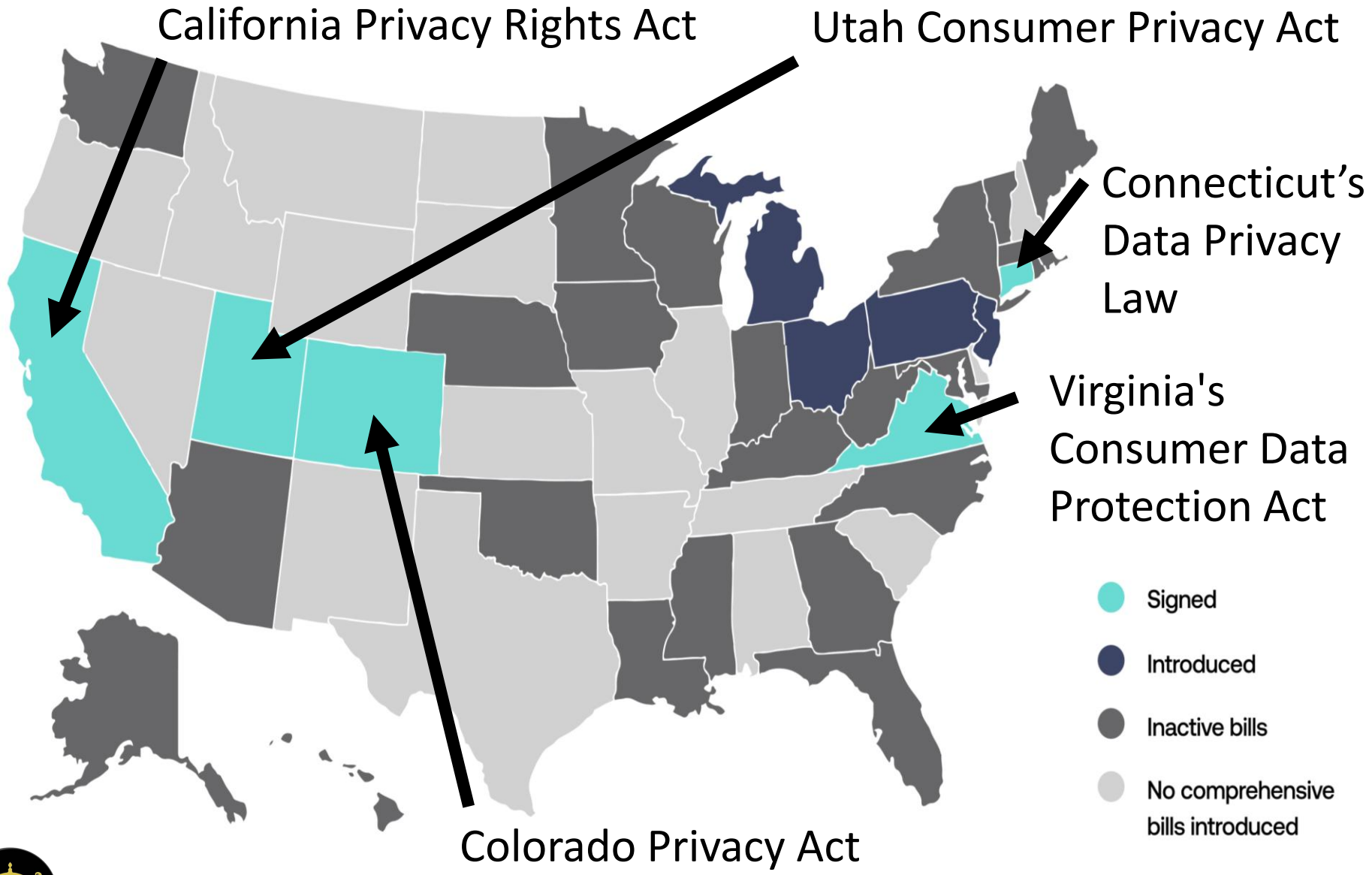
- Applies to all organizations processing the personal data of data subjects who reside in EU or the controller/processor has establishment in EU.
  - Focus on geography rather than citizenship.
- It does not apply to
  - Processing covered by the Law Enforcement Directive.
  - Processing for national security purposes.
  - Processing carried out by individuals purely for personal/household activities.
- It harmonizes data privacy laws across Europe.
  - Directly binding and applicable in all member states.



Laws in the USA

- The right to privacy is not explicitly stated anywhere in the Bill of Rights.
- Despite numerous proposals, no one comprehensive federal law governs data privacy in the U.S. yet.
  - The American Data Privacy Protection Act (ADPPA) has made it the furthest along the legislative process.
- Federal laws that govern the collection of specific (rather than general) information online:
  - The Federal Trade Commission Act (FTCA)
  - The Children's Online Privacy Protection Act (COPPA)
  - The Health Insurance Portability and Accounting Act (HIPAA)
  - The Gramm Leach Bliley Act (GLBA)
  - The Fair Credit Reporting Act (FCRA)
  - The Family Educational Rights and Privacy Act (FERPA)

State Level Privacy Laws



GDPR

- Replaces the Data Protection Directive 95/46/EC.
  - Not directly applicable, member states must enact them into national law.
- Regulations must be adopted word-by-word.
  - Stronger national law can be made (but not weaker).
- Enforcement date: 25 May 2018.
  - After this non-compliance can imply fines.
- Aims to give control back to Data Subjects over their personal data.
- Protects the fundamental right of privacy and data protection of Data Subjects.

Rights of the Data Subject

Rights 1/4

- Right to Access
  - The personal data and the privacy notice.
  - This must be provided for free within 1 month unless the request is unfounded, excessive or repetitive.
  - If the asked information is of large amount, the controller can ask the reason of access.

- Right to Data Portability
  - Data subjects can obtain and reuse their personal data for their own purposes across different services.
  - Data must be provided in common/open formats (XML, CSV, etc.).

Rights 2/4

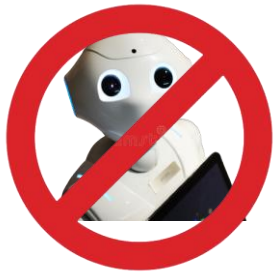
- Right to Rectification
  - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.

- Right to Erasure (Right to be Forgotten)
  - Request the deletion or removal of personal data.
  - Except if the data is needed to comply with a legal obligation, or for public health purposes in the public interest, or for public interest/statistical purposes, or to exercise a legal claims.

Rights 3/4

- Right to Object
  - Must stop processing personal data for direct marketing purposes immediately without exemptions or grounds to refuse.
  - Compliance with this right is not required if data is necessary for the performance of a public interest task.

- Right to Restrict Processing
  - Block or suppress processing of personal data.
  - Controller is permitted to store the personal data, but not process it.



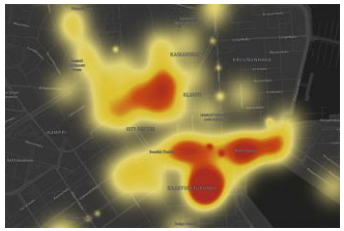
- Rights related to automated decisions and profiling
  - Right not to be subject to a decision which is based on automated processing.
  - Right to obtain an explanation of the decision and challenge it.
  - Does not apply to processing authorized by the law.

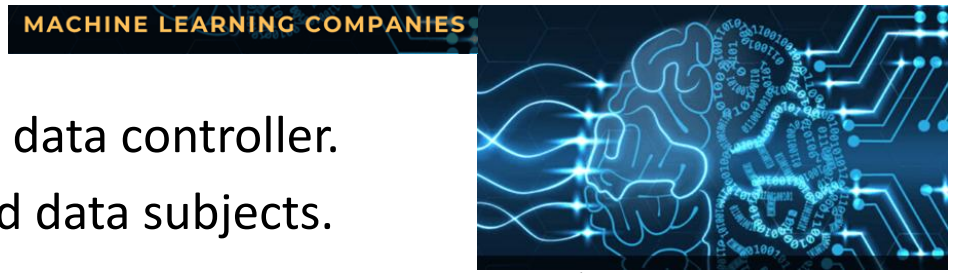
Wrongs

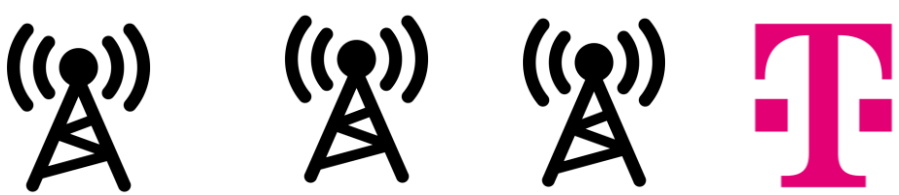
- A breach leads to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
- Report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected. Notification must include the likely consequences of the personal data breach.
- Must be sent within 72 hours after the organization becoming aware of the breach.
- Failing to send the notification can result in 10 million euro fine!

Actors

- Data Controller
  - Determines the purposes and means of the processing of personal data.
  - Not relieved of its obligations when a processor is involved.
- Data Processor
  - Processes data on behalf of the data controller.
  - Liable both to the controller and data subjects.
- Data Subject
  - Living individuals whose data is processed.
  - They are the data owners.

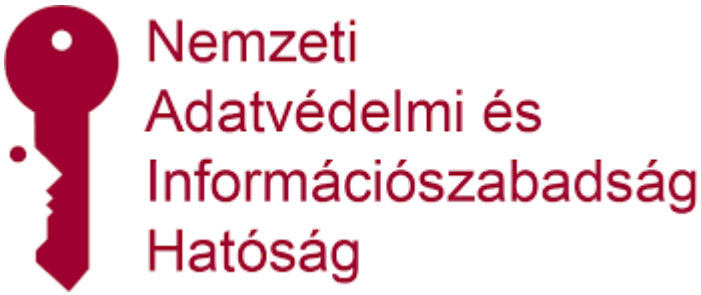






Data Protection Authority

- Investigate complaints, sanction administrative offences.
- Each member state establishes one DPA.
  - They obliged to deal with the complaints and application received from Data Subjects.
- European Data Protection Board (EDPB) coordinate them.
  - Providing general guidance to clarify the law and promote a common understanding.
  - Advising the European Commission on any issue related to the protection of personal data and new proposed EU legislations.
  - Ensuring consistency of the activities of National Authorities on cross border matters and settling disputes arising between them.



Data Protection Officer

- DPO ensures that the organization processes the personal data of its staff, customers, providers or any data subjects in compliance with the applicable data protection rules.
  - Not personally responsible for non-compliance, the liability remains with the controller or processor.
  - Can be internal or external.
- Needed for organizations if
  - The processing is carried out by a public authority.
  - Core data processing operations require regular and systematic processing of data subjects on a large scale.
  - Data processing operations require large scale of sensitive data or data relating to criminal offences.

Personal & Sensitive & Confidential Data

Personal Data

- "Personal data are any information which are related to an identified or identifiable natural person."
  - Identified: within a group of persons, the person is "distinguished" from all other members of the group.
  - Identifiable: it is possible to identify.
- Identifiers are related to physical, physiological, genetic, mental, economic, cultural or social identity of the natural person.
  - E.g., height, profession, visited locations, purchased goods, watched movies.
- GDPR refers to all personal data as identifiers which together unambiguously identify a person in the given context.

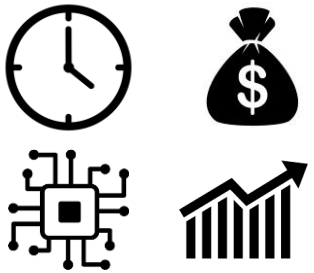
Identifiers

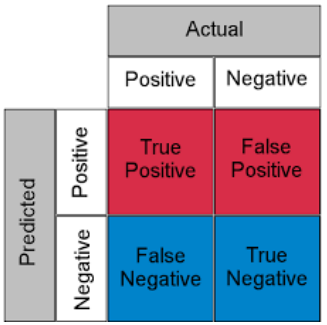
- Direct identifiers unambiguously identify a person.
  - E.g., social security number, multiple visited locations, titles like: “The Queen of England in 1980”.
  - The presence of direct identifiers is not necessary but sufficient condition of personal data.
- Indirect (quasi)identifier may ambiguously identify a person.
  - E.g., date of birth, single visited location, titles like “The Queen from England in 1980”.
  - Together, they can make a person identifiable.

- This distinction between direct and indirect identifiers is a bit blurred.
  - Full name in country vs in a classroom.

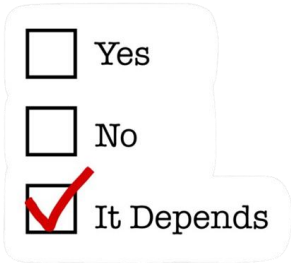
Identifiability

- "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."
- A person is identifiable, if there is a *plausible* attack reidentifying the person and it has a *reasonable* chance of succeeding.
  - Plausible: the attacker has enough motivation to launch the attack.
  - Chance of succeeding: the success probability of the attack.





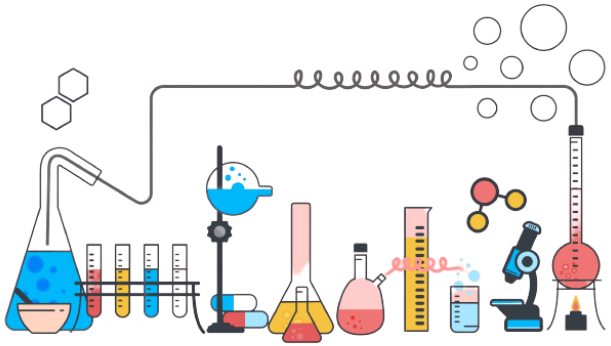
- There are no explicit pre-defined thresholds of plausibility and reasonable chance beyond which piece of information is considered as "personal"; they strongly depend on the context.



Sensitive Data

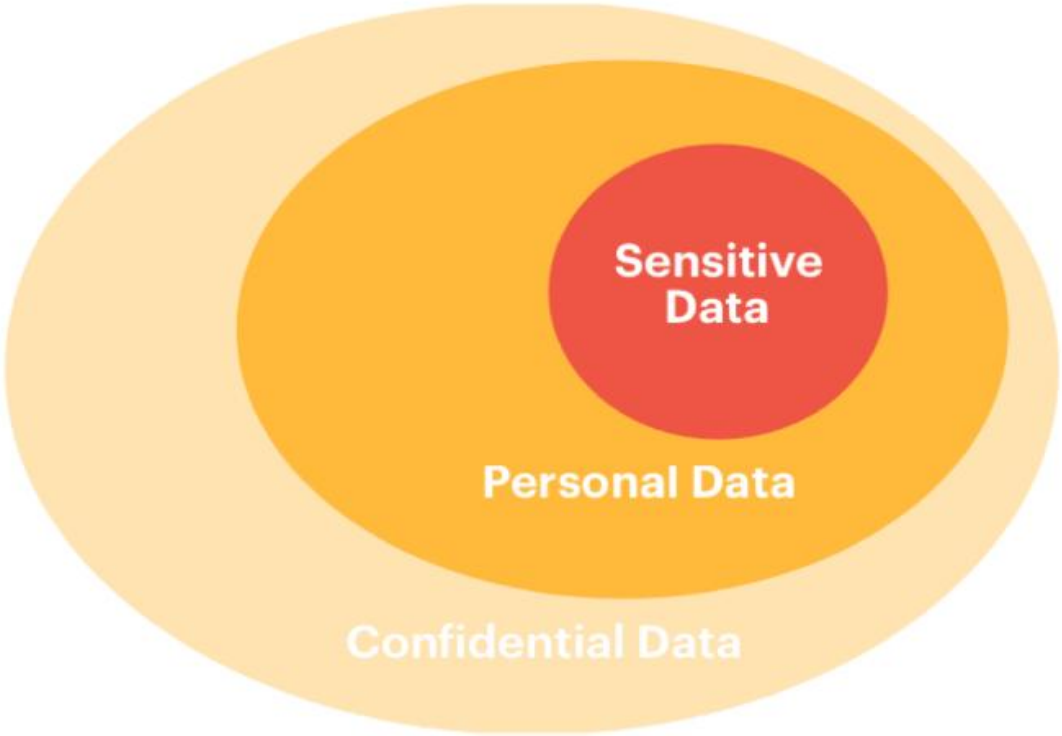
- Special categories of personal data which reveals:
  - Racial or ethnic origin
  - Political opinions
  - Religion or philosophical beliefs
  - Trade union membership
  - Genetic/biometric data
  - Data about health, sex life, sexual orientation

- Processing and storing of sensitive data is prohibited unless:
  - Used for research or in public health or for preventive medicine.
  - Data subject provide explicit consent.
  - Data subject made it already public.
  - Needed for legal claims.
  - Needed to protect the vital interests of the data subject or another natural person.



Confidential Data

- Confidential data is a broad categorization of any information of commercial value in which disclosure, alteration or loss could cause substantial harm to the competitive position of the data holder.
  - Personal data could also be confidential.



Examples

- Identifiability
  - Source Code
    Unique coding style might reveal the identity of the developer.

```
if len(response.data) != 0:
    ltdate = response.data[0]['created_at']
    ltdate2 = datetime.strptime(ltdate,'%a %b %d %H:%M:%S +0000 %Y'
    today = datetime.now()
    howlong = (today-ltdate2).days
    if howlong < daywindow:
        print i.screen_name, 'has tweeted in the past' , daywindow,
        totaltweets += len(response.data)
        for j in response.data:
            if j.entities.urls:
                for k in j.entities.urls:
                    newurl = k['expanded_url']
                    urlset.add((newurl, j.user.screen_name))
    else:
        print i.screen_name, 'has not tweeted in the past', daywind
```

MAYBE!

- Sensitive Data
  - Face
    Machine Learning models can predict the sexual orientation.

Principles of GDPR

Principles 1/3

- Storage limitation
  - Stored for only as long as required, as specified in the privacy policy.

- Purpose limitation
  - Personal data is collected for specified, explicit and legitimate purposes and not further processed beyond the specified purposes.

- Data minimisation
  - collected personal data is relevant and limited to what is necessary in relation to the purposes.

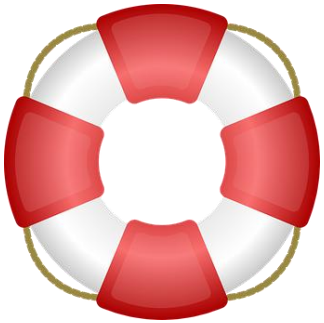
Principles 2/3

- Accuracy
  - Personal data is kept up to date; every reasonable step must be taken to ensure accuracy; any inaccuracies must be removed.
- Integrity and confidentiality
  - Ensures appropriate security of the personal data, including the protection against unauthorized access, modification, and against accidental loss, destruction, or damage.
- Accountability
  - The controller and processor shall be responsible for and be able to demonstrate compliance with the all principles.

- Lawfulness, fairness and transparency

Lawfulness, Fairness and Transparency

- Personal data is processed lawfully, fairly and in a transparent manner in relation to the Data Subject if at least one of the following condition holds:
  - Processing is *necessary for the contract* to which the Data Subject is party.
  - Processing is necessary for *compliance with a legal obligation* of the Data Controller.
  - Processing is necessary to *protect the vital interests* of the Data Subject or another person.
  - Processing is necessary for the performance of a *task carried out* in the public interest or in the exercise of *official authority*.
  - Processing is necessary for the purposes of the *legitimate interests* pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.



Examples

- Organizers of a conference compile a list of invitees from LinkedIn.
  - Can they send them invitations?

- A company stores the list of visited pages per visitor without any direct identifier.
  - Can they rely on “legitimate purposes” as a lawful basis of processing?

- Tracking is unlawful under GDPR without the consent of the Data Subject.

Consent

- Besides the previous six cases, personal data is processed lawfully if the data subject has given a consent.

Considered
Reversible
Informed
Specific
Participatory

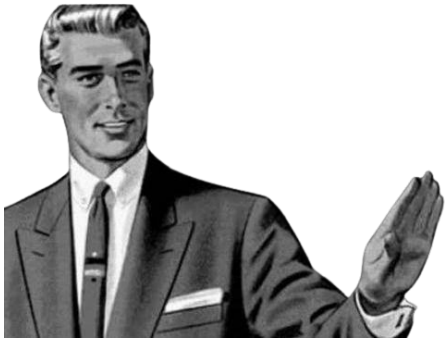
- "Any *freely given*, *specific*, *informed* and *unambiguous* indication of the data subject's wishes by which he or she, by a statement or by a *clear affirmative action*, signifies agreement to the processing of personal data relating to him or her."

- Accountability: controller must be able to demonstrate that it obtained a valid consent.
  - Asking invalid consent could be fined up to €20 million, or 4% of the total worldwide annual turnover, whichever is higher.

Freely Given
Reversible
Informed
Enthusiastic
Specific

Freely Given Consent

- Consent means giving people genuine choice and control over how you use their data.
  - Without a real choice, consent is invalid.

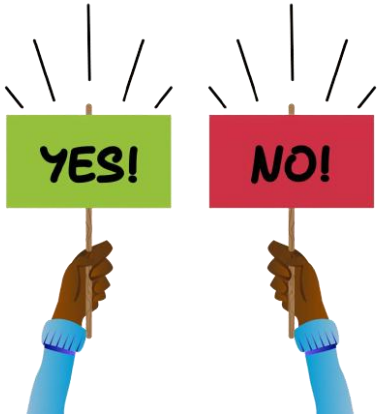


- People must be able to refuse consent without detriment and must be able to withdraw consent easily at any time.

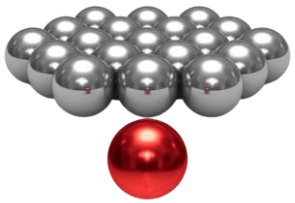
- When is consent not freely given?
  - As a condition of a service when it is not necessary for that service.
  - Data controller is in a position of power over the data subject, e.g., employer and employee.
  - …

Specific Consent

- The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language (easy-to-understand).
- Consent must include:
  - The controller's identity
  - The right to withdraw at any time
  - The purpose of processing
  - The processing activities



- Separate consent is needed for different processing operations, unless this would be unduly disruptive or confusing.
  - Single consent is sufficient for compatible purposes.



- Consent for research purpose does not need to be as specific, e.g., general areas of research are sufficient.

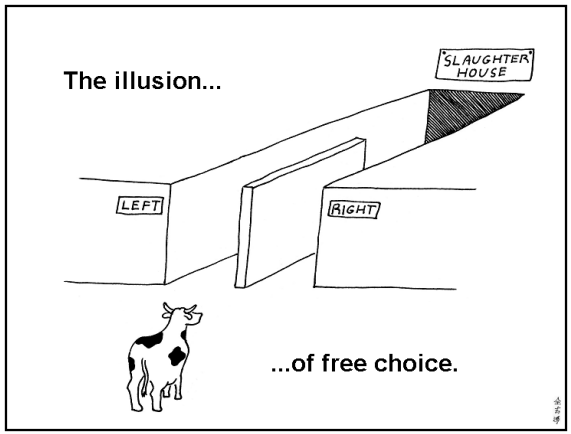
Unambigious Consent

- Opt-in statement: asks the individual actively to agree (by default, his data is not used).
  - Privacy by Default.
- Opt-out statement: asks the individual to object if he/she disagrees (by default, his data is used).
  - Unlawful under GDPR.

- Consent requires clear affirmative action.
  - Explicit: it must be expressly confirmed in words, rather than by any other positive action.
  - Implicit: consent informed from actions.

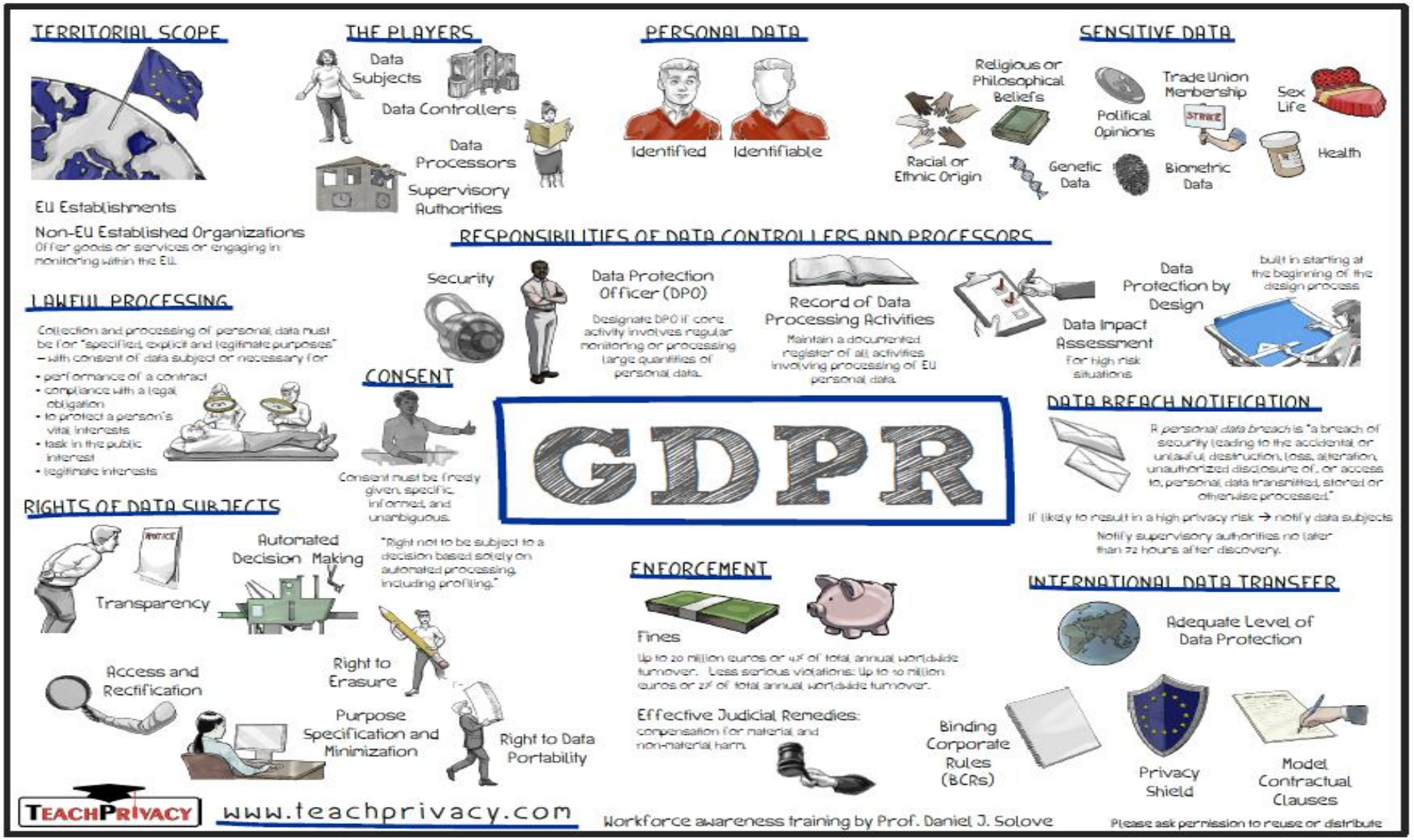
Examples

- Free Consent
  - An online furniture store requires customers to consent to their details being shared with other homeware stores as part of the checkout.



- Unambigious Consent
  - Consider the patient who walks into a doctor's office and tells the doctor all about the medical ailment from which he or she is suffering, while the doctor enters notes into his computer.

Summary


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
Religious or Philosophical Beliefs
Political Opinions
Trade Union Membership
Sex Life
Racial or Ethnic Origin
Genetic Data
Biometric Data
Health
RESPONSIBILITIES OF DATA CONTROLLERS AND PROCESSORS
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
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 Protection by Design
built in starting at the beginning of the design process
Data Impact Assessment
For high risk situations
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.
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
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
www.teachprivacy.com
Workforce awareness training by Prof. Daniel J. Solove
Please ask permission to reuse or distribute

Other Related Laws

The Digital Markets Act

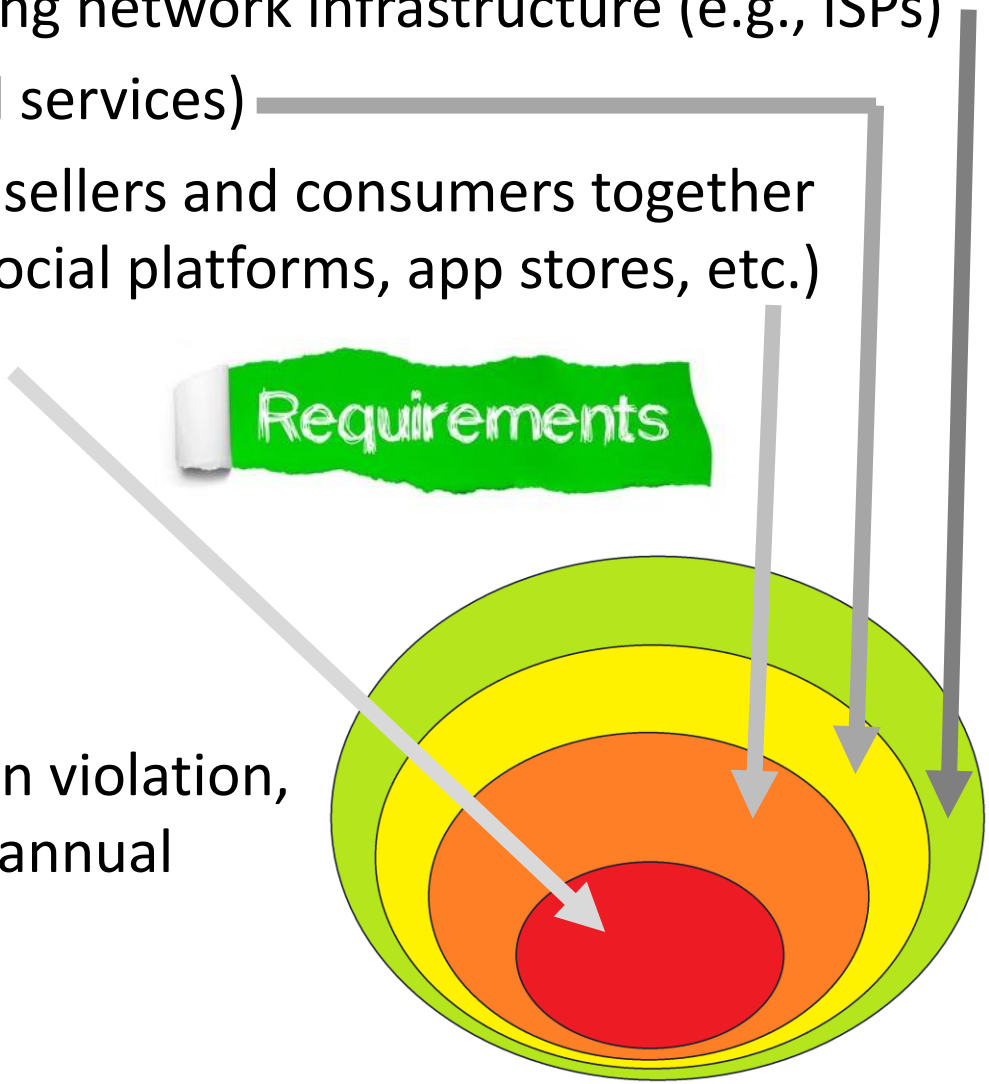
- DMA prevents the largest digital platforms (e.g., Facebook, Apple, Microsoft, Amazon, Google), known as “gatekeepers”, from imposing unfair conditions on their competitors.
  - A company is considered a gatekeeper if it has a strong economic position, significant impact on the EU market, and is active in multiple EU member states.
- Violation of the DMA may result in fines up to 10% of annual global turnover or up to 20% in the case of repeated violations. What’s more, repeated violations may result in non-financial remedies, such as forced divestitures.
  - Published on 12 October 2022.
  - Entered into force on 1 November 2022.
  - Apply from 2 May 2023.

Digital Services Act

- Addresses illegal and harmful content by compelling platforms such as Google and Facebook to remove content that doesn't meet certain standards.
- The primary principle is "what is illegal offline must be illegal online," according to the Council of the EU.
  - Entered into force on November 16, 2022.
  - Different provisions of the law will become effective at different times.
  - Fully into force on February 17, 2024.

DSA Requirement Tiers

- Intermediary services offering network infrastructure (e.g., ISPs)
- Hosting services (e.g., cloud services)
- Online platforms that bring sellers and consumers together (i.e., online marketplaces, social platforms, app stores, etc.)
- Very large online platforms (i.e., reaching more than 10% of the 450 million consumers in Europe)



- If a business is found to be in violation, it may be fined up to 6% of annual global turnover during the preceding financial year.

Take Away

- GDPR is a general regulation valid across all EU states.
- It specifies the fundamental right of data protection.
- GDPR has a general definition of personal data, i.e., what is it and who is identifiable depends on the context/attacker.
  - There are six type of sensitive data, which enjoy stronger protection.
- It has seven principles, and personal data can be processed only if one of the six conditions apply (one of which is consent).
- Legal compliance is not the only motivation for privacy protection, trust is a competitive differentiator.

Control Questions

- What are fundamental rights?

  In what two ways can they be limited?

- What is personal data

  according to the GDPR?

  Explain the words

  in the definition!

- Who are the actors in GDPR?

  What are the DPA, DPO,

  and the EDPB?

References

- GDPR
  - Legitimate interest
  - Personal data
  - Individual rights
  - Processing principles
  - DPO
  - Consent (TED)

- Statistics
- Privacy Laws Worldwide

Video

https://www.youtube.com/watch?v=GVU3nmaRqjE