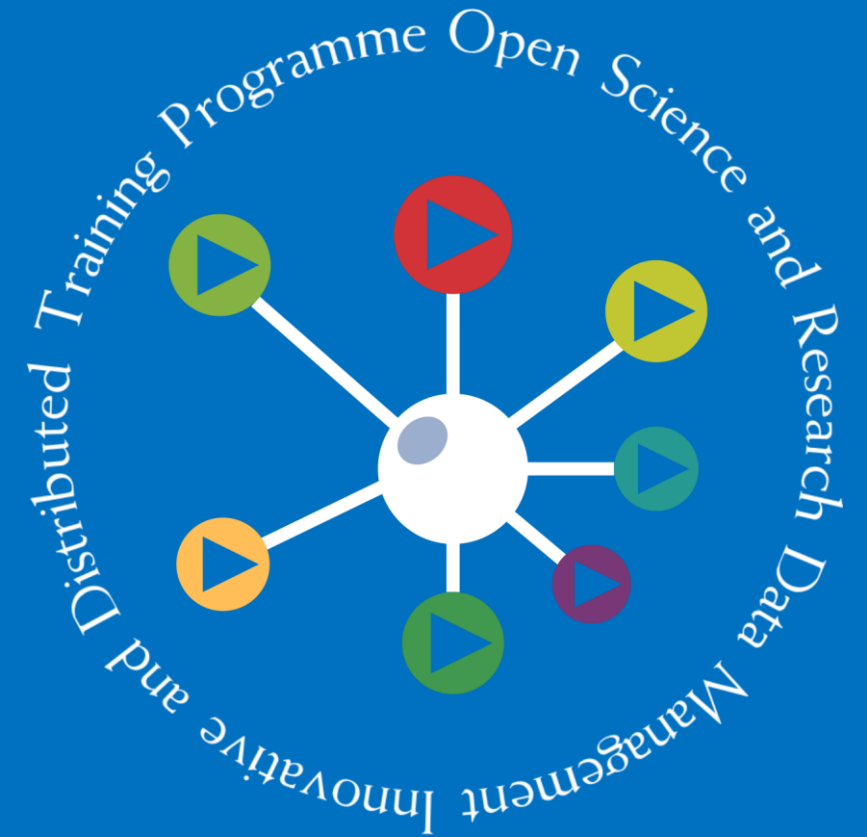


Data Governance, Compliance, and Ethics

Privacy and Data Protection

This module is part of
Early-Stage Researchers' Training Week
within the TrainRDM project

National College of Ireland
Dublin, Ireland



Module Aims And Objectives



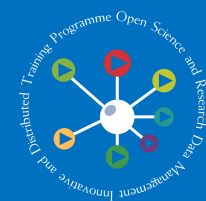
🌐 This module aims to provide learners with the knowledge and skills around the complex issues of data management and governance in an organisational context, including ethical and compliance issues that these present. Learners will explore the ethical, legal, and social implications of using data-driven technologies such as big data, analytics, internet of things, and machine learning. The students will learn how to establish processes and systems that consider best practices for data governance and adhere to ethical and regulatory requirements for data handling.



Minimum Intended Module Learning Outcomes

- ❖ LO1 Demonstrate critical understanding of the governance and **regulatory frameworks associated with the key data lifecycle stages** for an effective management of data assets.
- ❖ LO2 Demonstrate critical **awareness and interpretation of the data privacy and data protection regulatory landscape** in socio-technical environments.
- ❖ LO3 Critically analyse and evaluate the main ethical, **legal**, and social **implications of using data-driven technologies**.
- ❖ LO4 Investigate and appraise the interplay of fairness, accountability, and transparency in algorithmic decision-making systems and demonstrate awareness of technical solutions to enhance these concerns.

Agenda



Topic	Lecture Topic	Lecture Detail
4	Privacy and Data Protection I	Brief history of human rights; Privacy and confidentiality; Sources of rights: Universal declaration of human rights, European Convention on Human Rights, EU Charter of Fundamental Rights; Types of EU legislation
5	Privacy and Data Protection II	National law; General Data Protection Regulation Scope; Personal data; Legitimate bases for data processing; Data protection principles; Data subject rights; Privacy by design and by default
6	Privacy and Data Protection III	Data protection impact assessment; Issues of consent; Supervision and enforcement; Data protection in practice including international transfers, surveillance, cloud computing, and auditing

Privacy and Data Protection (Part I)

The Right To Privacy - History and European Institutions



European Data Protection Origins

"No matter how much an authority or company wants us to trust them, data about us in the wrong hands can seriously harm us."

Tim Clements (Purpose and Means)

Comprehensive data protection laws are essential for protecting human rights

25th May 2023 – 5th year anniversary of the GDPR

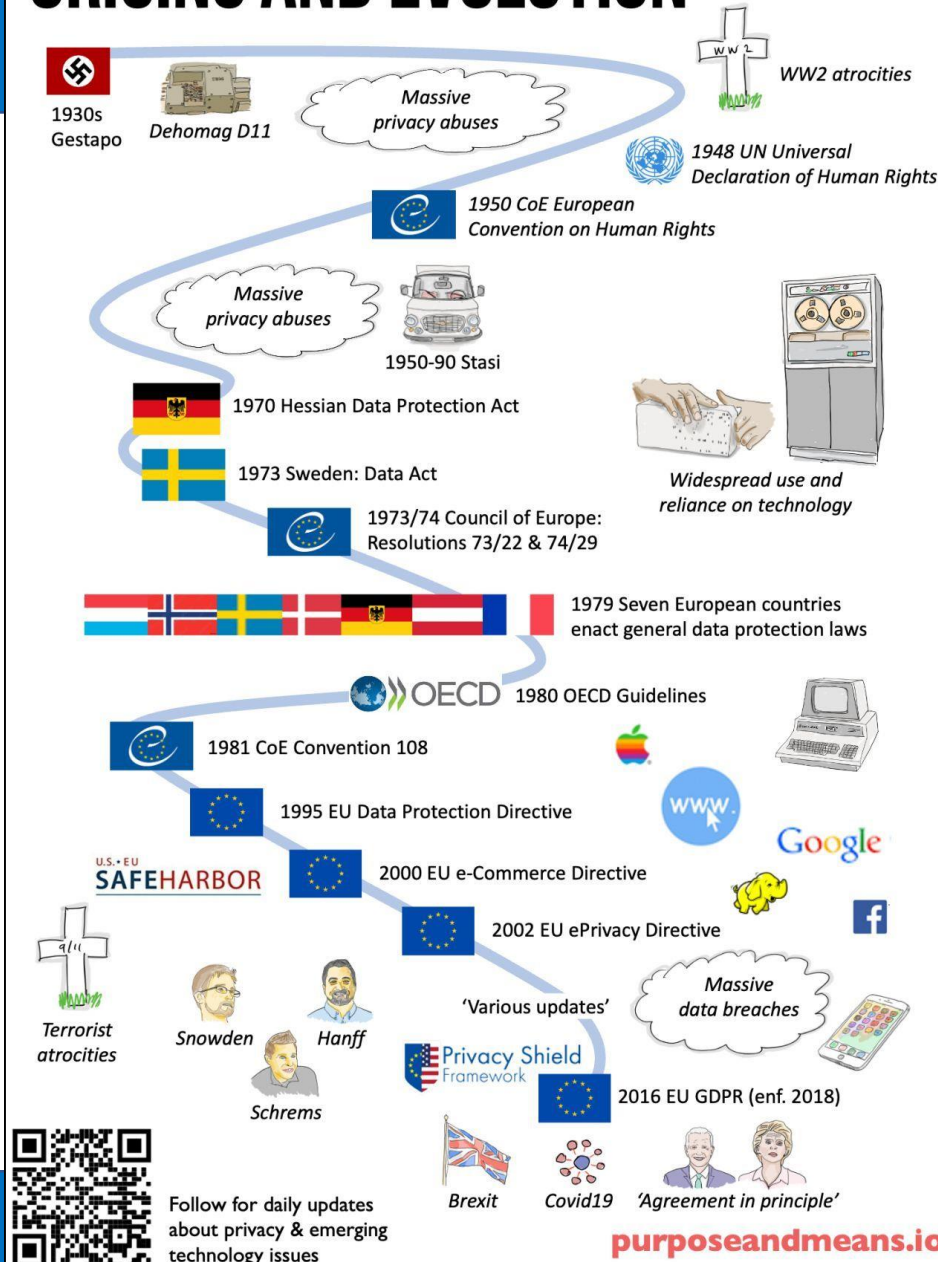
Example of events:

1945 – establishment of the United Nations

1948 – declaration of the **Universal Declaration of Human Rights**, a milestone document in the history of human rights

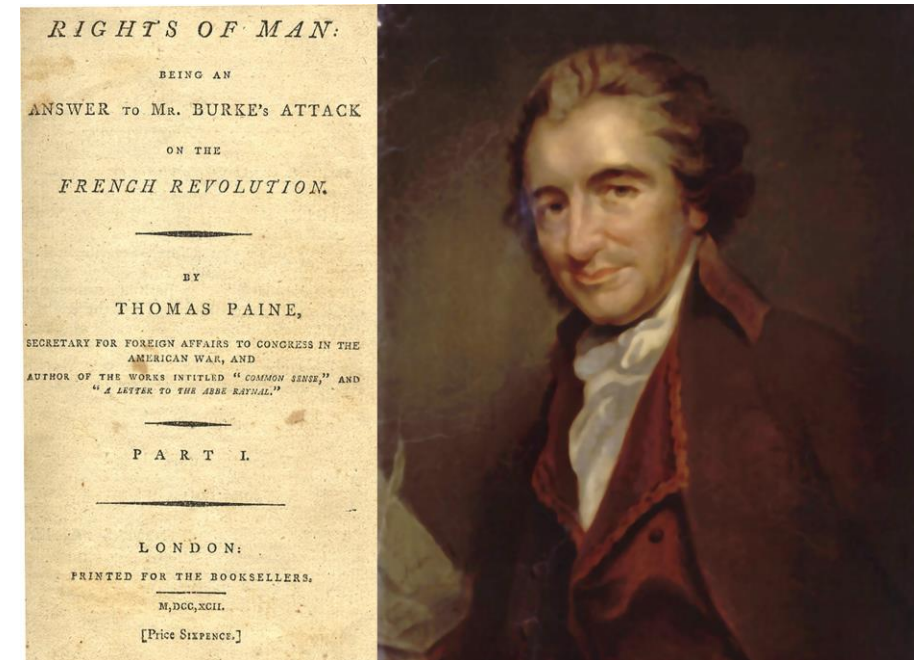


EUROPEAN DATA PROTECTION ORIGINS AND EVOLUTION



A Short History of Human Rights

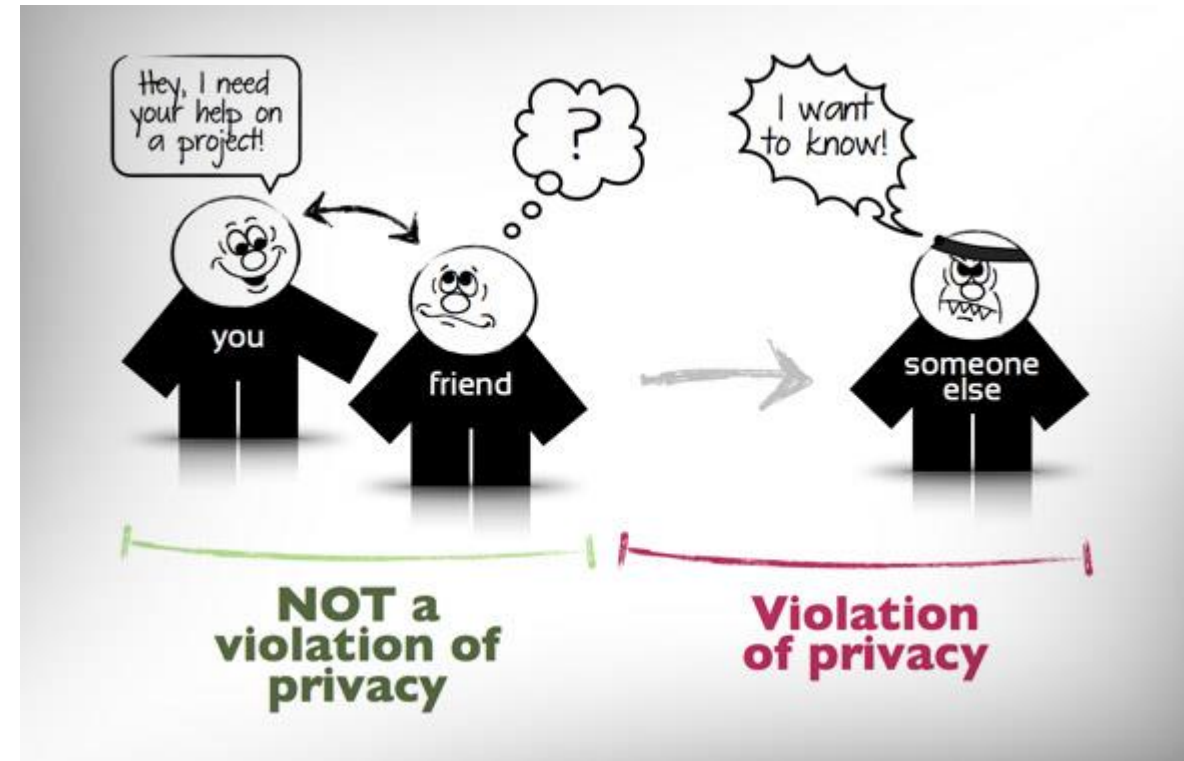
- ✿ Privacy underpins human dignity
- ✿ Universal human rights are a relatively new concept but it does have its antecedents in documents throughout history:
 - ✿ Magna Carta (1215)
 - ✿ English Bill of Rights (1689)
 - ✿ French Declaration on the Rights of Man and Citizen (1789)
 - ✿ US Constitution and Bill of Rights (1791)
- ✿ Some writers were very influential in the development of the concept (e.g., Thomas Paine and the Rights of Man(1791)) but it was not until the 20th century that the concept came into its own).
- ✿ Problem: Many of these excluded different groups, thus, **they were not universal.**



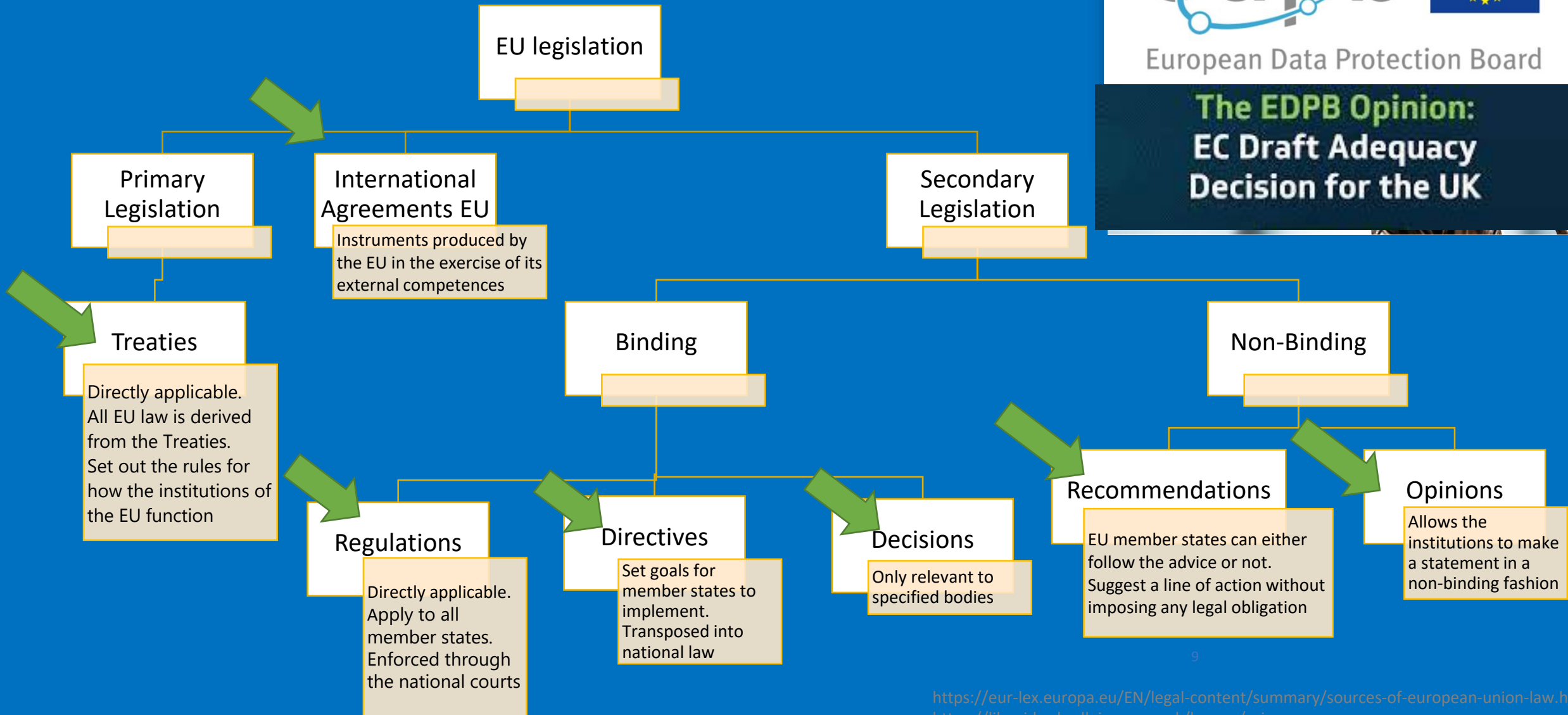
“popular political revolution is permissible when a government does not safeguard the natural rights of its people”

Concept of Privacy

- ❖ **Right of Privacy** can be defined as the right of a person to enjoy his own presence by himself and decide his boundaries.
- ❖ Individual has a right to limit sharing his personal information with other individuals or entities or the media.
- ❖ Personal information is a form of personal property to an individual.



Types of EU legislation



European Data Protection Board

The EDPB Opinion:
EC Draft Adequacy
Decision for the UK

The Right to Privacy



🌐 The right to privacy is guaranteed both in:

1. The Constitution (National basic law)
2. European Level

🌐 1948: UN Universal **Declaration** of Human Rights

🌐 1953: European **Convention** on Human Rights (ECHR)

🌐 1958: EU **Charter** of Fundamental Rights

The Right to Privacy



🌐 The right to privacy is guaranteed both in:

1. The Constitution (National basic law)
2. European Level

🌐 1948: UN Universal **Declaration** of Human Rights

🌐 1953: European **Convention** on Human Rights (ECHR)

🌐 1958: EU **Charter** of Fundamental Rights

The Right to Privacy in the Universal Declaration Of Human Rights

❖ After WW2, fundamental rights should be attributable to individuals irrespective of their country of origin

❖ Adopted by the UN General Assembly in Paris on 10 December 1948 proclaims the inalienable rights of all human beings

❖ The Universal Declaration of Human Rights serves as a foundational document for international human rights; it sets out for the first time fundamental human rights to be universally protected

❖ It is composed of 30 articles

❖ **Article 12** “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”



The Right to Privacy



✿ The right to privacy is guaranteed both in:

1. The Constitution (National basic law)
2. European Level

✿ 1948: UN Universal **Declaration** of Human Rights

✿ 1953: European **Convention** on Human Rights (ECHR)

✿ 1958: EU **Charter** of Fundamental Rights

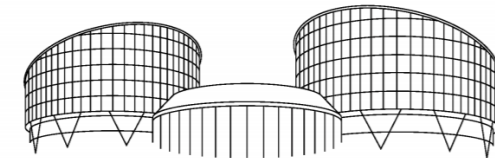
The Right to Privacy in the European Convention on Human Rights

1/2

- ✿ Established in 1950 and entered into force in 1953
- ✿ Based on the UN Universal Declaration of Human Rights.
- ✿ **Enforced by the European Court of Human Rights** (ECtHR) a.k.a. Strasbourg Court
- ✿ Article 8 **Right to respect for private and family life** states that:

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

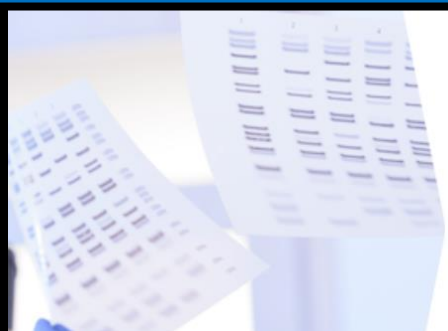
Guide on Article 8
of the European Convention
on Human Rights

Right to respect for private and family life,
home and correspondence

Implementation of the European Convention on Human Rights



- The European Court of Human Rights a.k.a. the Strasbourg Court, is an international court of the Council of Europe that **interprets the European Convention on Human Rights**
- Judgements of the Court legally bind countries to stand by its rulings.



DNA records of innocent people destroyed after privacy complaint

Two men from Sheffield had DNA samples taken by the police. Criminal charges against them were dropped. However, under British law the police could retain their DNA forever. The Strasbourg court ruled that keeping DNA records of innocent people breached their right to privacy.

THEMES: Right to privacy  United Kingdom



Justice for woman whose private health data was leaked to journalists

Gitana Biriuk took successful legal action against a newspaper that disclosed her HIV status. She only received a small amount in damages because of legal limits on what could be awarded. The European court ruled that these limits failed to protect Gitana's right to privacy. By the time of the judgment, Lithuania had removed the upper limit on compensation awarded by its courts in such cases.

THEMES: Right to privacy  Human rights and health  Lithuania



Privacy reforms after retired couple had their phone tapped

Jacques and Janine Huvig were a retired couple who had run a fruit-and-vegetable business. Police tapped their phone and listened to their conversations. At the time, investigators had almost limitless powers to tap the phones of almost anyone for almost any reason. The European court ruled that there must be clear legal limits and safeguards to protect people's privacy – leading to a change in...

THEMES: Right to privacy  France

The Right to Privacy



✿ The right to privacy is guaranteed both in:

1. The Constitution (National basic law)
2. European Level

✿ 1948: UN Universal **Declaration** of Human Rights

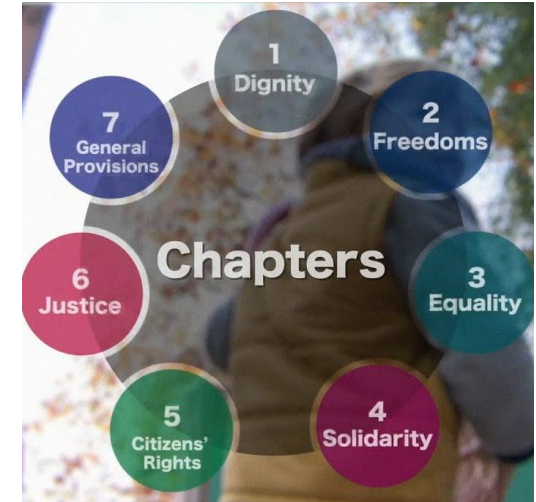
✿ 1953: European **Convention** on Human Rights (ECHR)

✿ 1958: EU **Charter** of Fundamental Rights

The Right to Privacy in The Charter Of Fundamental Rights



- ✿ The Charter of Fundamental Rights of the European Union brings together the most important personal freedoms and rights enjoyed by citizens of the EU into one legally binding document (**overarching framework for human rights in the EU**)
- ✿ The Charter was declared in 2000 and came into force in December 2009
- ✿ The Charter is **interpreted by the Court of Justice of the European Union (CJEU)**
- ✿ It is based on the EU Treaty, CJEU case law, member states' constitutional traditions, and the European Convention on Human Rights
- ✿ The Charter however **addresses some modern issues** that are not included in the ECHR (for example, human cloning, and data protection).



•Chapter 2: Freedoms (Art. 6 – 19)

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and communications.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Implementation of The Charter Of Fundamental Rights



- ✿ Rights provisions can be enforced through decisions in national courts or ultimately European Court of Justice
- ✿ Fundamental Rights Agency provides a database of relevant court cases.
- ✿ Under Article 8 (Protection of Personal Data), among some cases listed

CJEU Case C-311/13 / Opinion

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems

Policy area: Information society

Deciding body type: Court of Justice of the European Union

Deciding body: Advocate General

Type: Opinion

Decision date: 19/12/2019

ECLI (European case law identifier): ECLI:EU:C:2019:1145

Privacy and Data Protection (Part II)

Key Provisions in the General Data Protection Regulation (GDPR)



The General Data Protection Regulation (GDPR)



- came into **effect in 25 May 2018** to replace the Data Protection Directive 1995
- harmonize data privacy laws across Europe
- applies to all organizations that handle personal data of EU residents
- adds new rights to individuals & new obligations to organizations (data controllers and processors)**
- can impose fines** up to €20 million or 4% of global turnover



Articles 1-3 cover the applicability of the GDPR

Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

3. For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

4. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

When Does the
GDPR Not Apply?



GDPR Material Scope

🌐 There are some cases where **GDPR will not apply**, this is depending on

- the **nature and circumstances** of the personal data processing,
- the **type** of personal data being processed,
- or **when** the data protection issue occurred,

the GDPR will not apply and **instead, another legal framework** concerning the regulation of the processing of personal data **may apply**.



🌐 For example

- if a data protection complaint or a possible **infringement** of the law relates to an incident **which occurred before the GDPR**
 - ➔ The Data Protection Acts 1988 – 2003
- After 25 May 2018, if the **processing** of personal data is carried out **for a law enforcement purpose**
 - ➔ The Law Enforcement Directive



Example– Material Scope Of The GDPR

Article 2 of the GDPR states that the **GDPR doesn't apply to a "purely personal or household activity."**:
Recital 18 of the GDPR provides some **examples of personal and household activities**:

- Personal correspondence
- Keeping an address book
- Social networking (as a private individual)

UK Ring doorbell court case

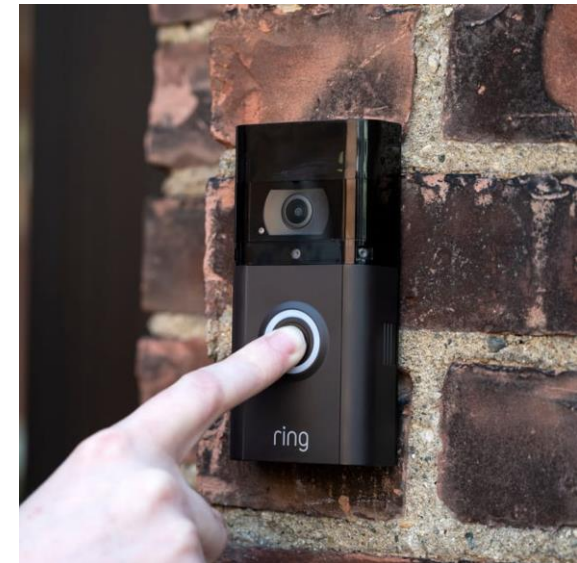
Camera doorbells allow you to see who is at your door when they press the button - as well as detect motion.

Dr Mary Fairhurst (the claimant) said she had to move out of her home because of the doorbell installed by neighbor Jon Woodward.

Mr Woodward (the defendant) had a Ring doorbell attached to the front door of his home in addition to a number of home security video devices set up around his home.

At the end of a court hearing, Judge Melissa Clarke said:

- Mr Woodward's use of the smart doorbell device and other personal CCTV items had breached data protection laws
- the images and video of Dr Mary are her personal data
- Mr Woodward had breached the Data Protection Act 2018 and UK GDPR and now faces a compensation fine of up to £100,000 for this breach



Personal Data

Art 4(1)

Personal data is **any information belonging to an identified or identifiable natural person**, i.e. an individual could be identified directly or indirectly with these data.

> a name, an identification number, location data, an online identifier, or factors such as physical, physiological, genetic, mental, economic, cultural or social that may lead to identifying a person.

E.g., Irish Supervisory Authority interpretation:

“The data was personal data as the complainant could be identified from it and it related to the complainant as an individual.”



Personal Data (Examples)

WHAT IS AND WHAT IS NOT CONSIDERED PERSONAL DATA
+ SPECIAL CATEGORY

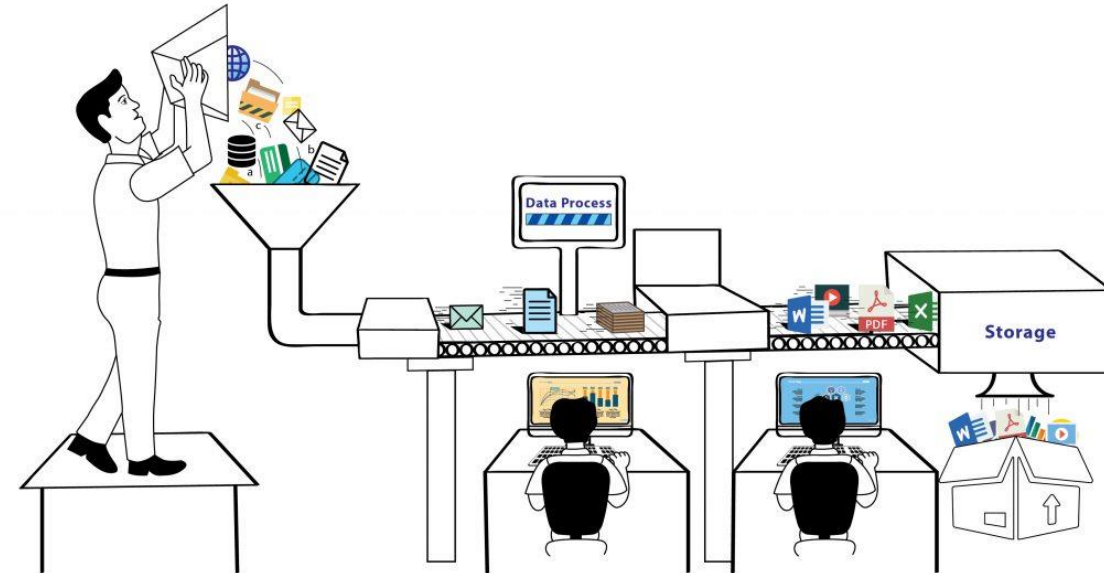
PERSONAL DATA	SPECIAL CATEGORIES	NOT PERSONAL DATA
• name • email address (name.surname@domain.com) • phone number • Internet Protocol (IP) address • home address	• criminal records • personal data related to racial or ethnic origin • medical records • religious or philosophical beliefs • trade-union membership • blood type • political stands...	• a company registration number; • an email address as info@company.com • anonymized data • information about legal entities • data related to a deceased individual

Processing of Personal Data

Art 4(2). Processing refers to any operation which is performed on personal data such as:

- Collection
- Organisation
- Storage
- Alteration
- Alignment Or Combination
- Use
- Erasure Or Destruction
- Restriction
- Recording
- Structuring
- Adaptation
- Retrieval Or Consultation
- Disclosure By Transmission, Dissemination Or Otherwise Making Available

Pseudonymised data is also in scope, while anonymized data is not.



Controller Vs. Processor

Art. 24-43

Controller: Any natural or legal person, public authority, agency or other body which alone or jointly with others determined the purposes and means of the processing of personal data.



- Responsible for managing the use of data
- Defines the how and why of personal data processing

Processor: A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

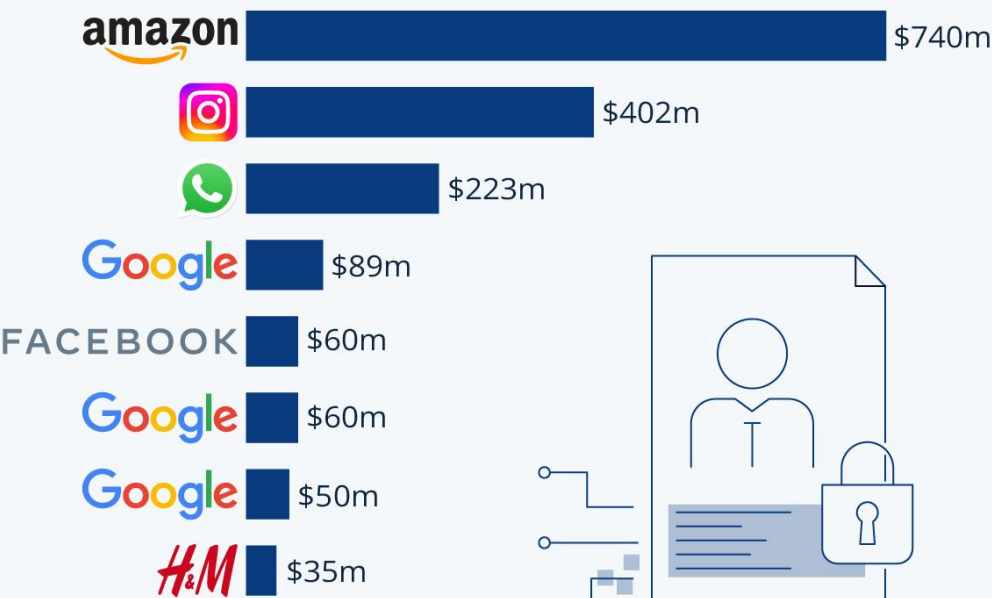


- Responsible for carrying out the actual processing
- Needs to maintain an audit trail of all processing activities

Administrative Fines

Big Tech, Big Fines

Highest fines for breaching one or more articles of the General Data Protection Regulation*

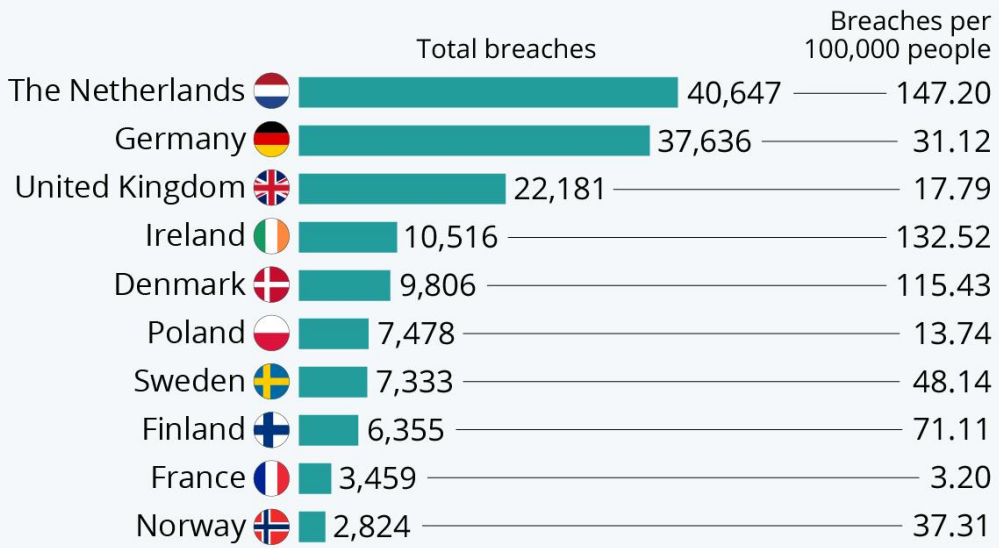


* Currency converted on Sep 6, 2022
Source: CMS GDPR Enforcement Tracker



The Countries With The Most GDPR Data Breaches

Personal data breaches notified per EEA jurisdiction (May 25, 2018 to Jan 27, 2020)*



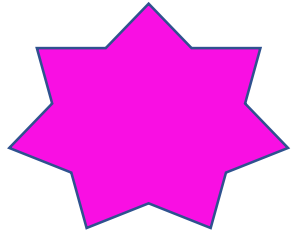
* EEA - European Economic Area (EU-28 + Norway, Iceland, Liechtenstein).
Source: DLA Piper



Key Data Protection Provisions in GDPR w.r.t. data protection measures



Data Protection Principles (Art. 5)



Data Subject Rights (Art. 13-22)



Privacy by Design and By Default –PbD (Art. 25)

Data Protection Principles

Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency

2. Purpose limitation

3. Data minimization

4. Accuracy

5. Storage limitation

6. Integrity and Confidentiality

7. Accountability

CONSENT
REQUIREMENTS UNDER
THE GDPR

AN FOIMAN INFOGRAPHIC WWW.FOIMAN.COM

MUST BE	MUST NOT
 Given by a statement or clear affirmative action	 Be inferred from silence, pre-ticked boxes or inactivity
 Freely given, specific, informed and unambiguous	 Make consent a condition for receiving a service unnecessarily
 Proven by the data controller	!?!? Use confusing unclear language
 Withdrawn as easily as it is given	 Bundle with other terms and conditions



Data Protection Principles

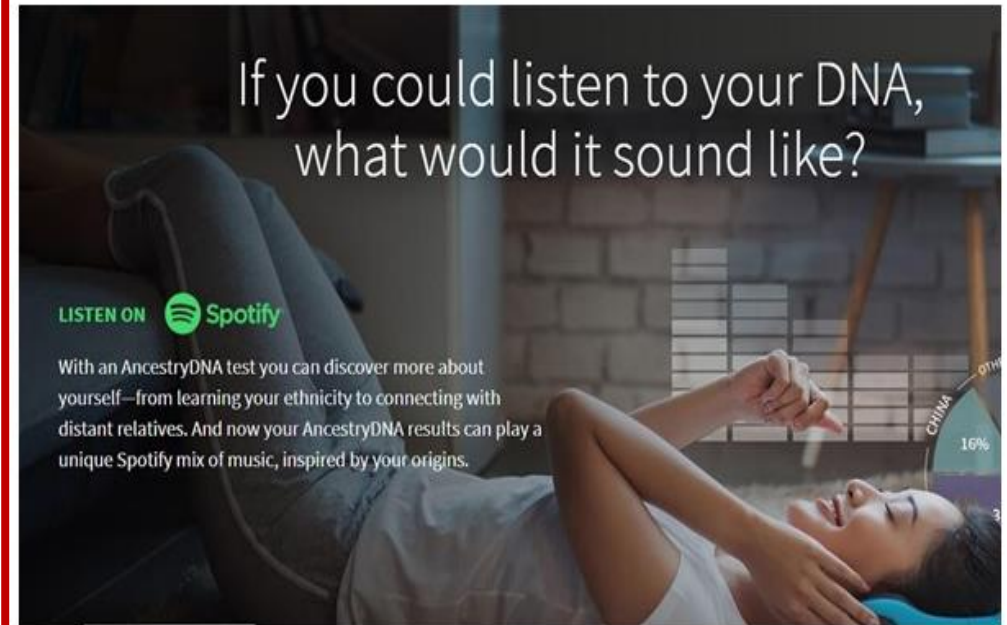


Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability

Spotify teams up with Ancestry to create playlists based on your DNA

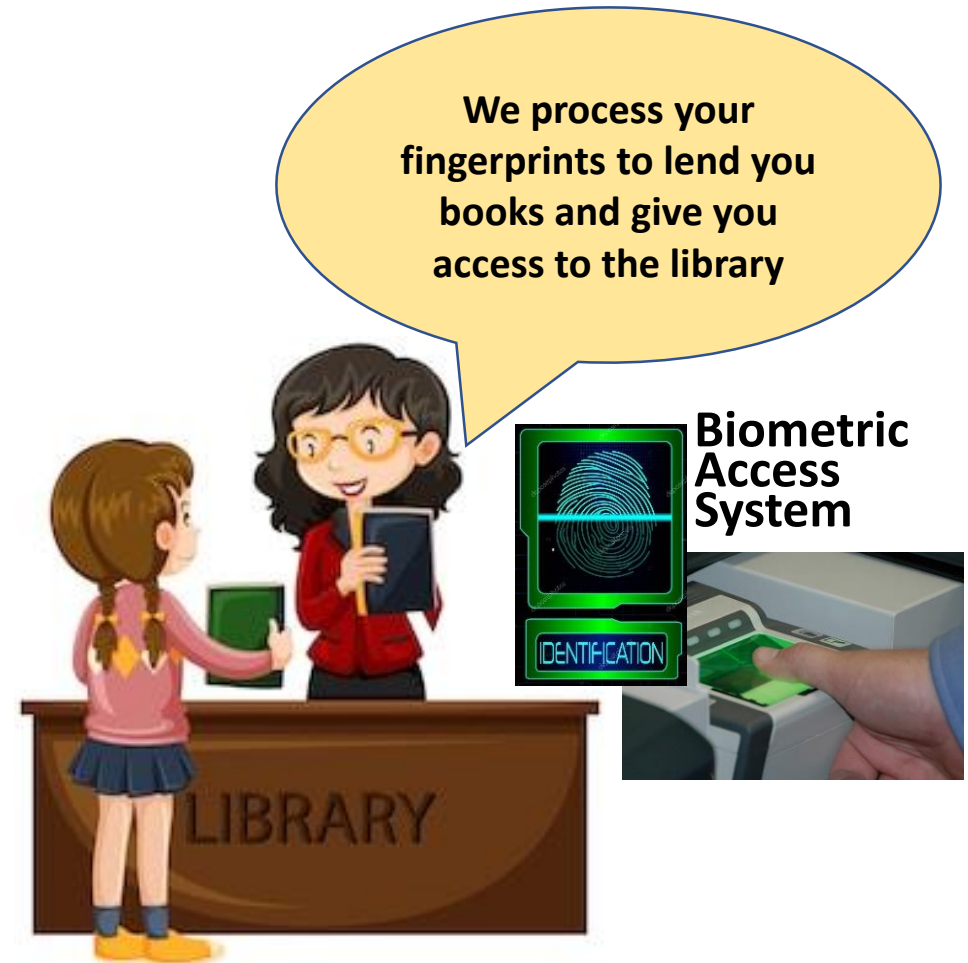
Tuesday, September 25, 2018 - 08:08 AM



Data Protection Principles

Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability



Data Protection Principles

Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability



Data Protection Principles



Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability



Data Protection Principles

Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability



Data Protection Principles



Art. 5-11 Data Protection Principles (DPRs)

1. Lawfulness, Fairness, and Transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and Confidentiality
7. Accountability



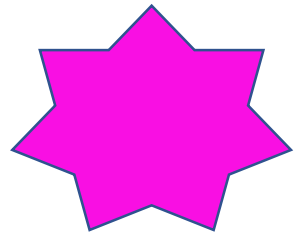
Key Data Protection Provisions in GDPR w.r.t. data protection measures



Data Protection Principles (Art. 5)



Data Subject Rights (Art. 13-22)



Privacy by Design and By Default –PbD (Art. 25)

Rights of the Data Subject

Art. 12-23



Key Data Protection Provisions in GDPR w.r.t. data protection measures



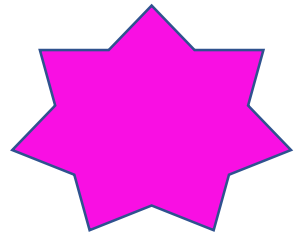
Data Protection Principles (Art. 5)



Data Subject Rights (Art. 13-22)



Privacy by Design and By Default –PbD (Art. 25)



Privacy by Design and By Default (Art. 25)



Art. 25 GDPR

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. ¹The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. ²That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. ³In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

“Implement appropriate technical and organizational measures ...”



Privacy by Design and By Default (Art. 25)



Ann Cavoukian, former Information and Privacy Commissioner of Ontario coined the Privacy by Design concept

1 PROACTIVE NOT REACTIVE; PREVENTATIVE NOT REMEDIAL



2 PRIVACY AS A DEFAULT SETTING

3 PRIVACY EMBEDDED INTO DESIGN

4 POSITIVE-SUM, NOT ZERO-SUM

5 END-TO-END SECURITY – FULL DATA LIFECYCLE PROTECTION

6 VISIBILITY AND TRANSPARENCY- KEEP IT OPEN

7 RESPECT FOR USER PRIVACY- KEEP IT USER-CENTRIC

EXAMPLE:

Girls Around Me mobile app shows where women who have checked-in on Foursquare are on a map.

➔ “Let’s stalk women” app



© 2011 Social Information Group

Transfers of Personal Data



Transfers of personal data to third countries or international organisations

- EU law requires that this is done in a way that is **“essentially equivalent”** to those required under EU law
- A third country refers to any country outside the European Economic Area (the “EEA”).
- Essentially EU provides for a tiered approach in providing such protections.

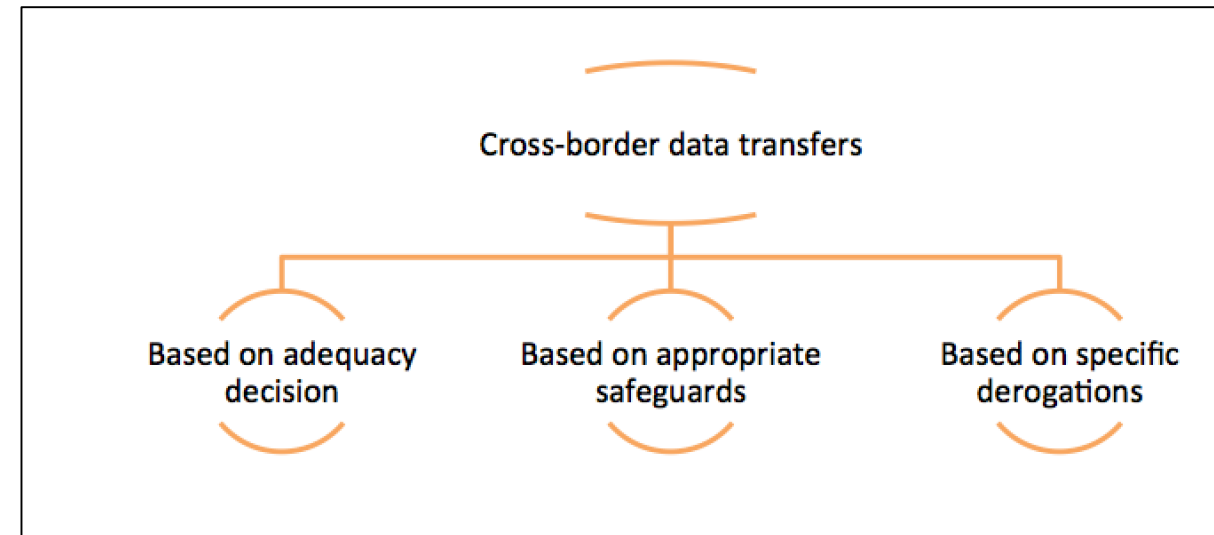
Article 44	–	General principle for transfers
Article 45	–	Transfers on the basis of an adequacy decision
Article 46	–	Transfers subject to appropriate safeguards
Article 47	–	Binding corporate rules
Article 48	–	Transfers or disclosures not authorised by Union law
Article 49	–	Derogations for specific situations
Article 50	–	International cooperation for the protection of personal data

A tiered approach

Transfers of Personal Data



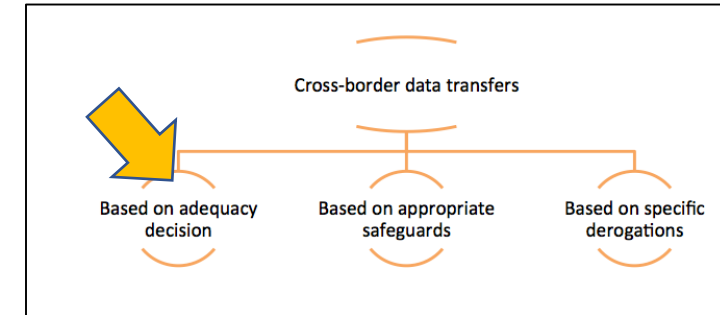
1. Transfers on the basis of an **adequacy decision** (Art. 45 GDPR)
2. Transfers subject to **appropriate safeguards** (Art. 46 GDPR)
3. **Derogations** for specific situations (Art. 49 GDPR)



Transfers Based On Adequacy Decision (Art. 45 GDPR)



✿ A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.



⇒ **Effect of adequacy decision: the transfer is the same as if was carried out within the EU (intra-EU transmissions of data)**

Adequate level of protection? After evaluating number of factors such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence of a data protection authority and binding commitments entered into by the country in respect of data protection

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the Law Enforcement Directive, and Uruguay **as providing adequate protection.**

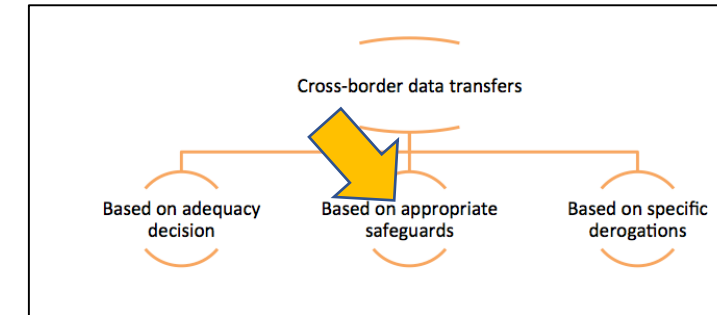
Transfers Subject To Appropriate Safeguards (Art. 46 GDPR)



✿ In the absence of an adequacy determination, personal data only transferred subject to “appropriate legally enforceable safeguards”

✿ These may include:

1. **Standard data protection clauses** contain **contractual obligations** on the Data Exporter and the Data Importer, and rights for the individuals whose personal data is transferred. Known as “standard contractual clauses (**SCC**)”. There are SCC between controller-controller and controller-processor.
2. **Binding Corporate Rules (BCRs)** — a legally binding **internal code of conduct** operating within a multinational group (approved by DPA, contain enforceable data subject rights, BCRs for controllers and processors) – further provisions on the use of BCRs are set out in GDPR Art. 47
3. an **approved code of conduct** pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights;
4. an **approved certification mechanism** pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects’ rights.



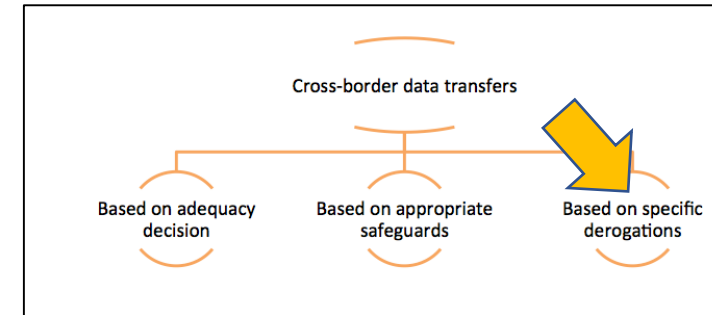
Transfers based on Specific Derogations (Art.49 GDPR)



❁ **Derogations are exemptions** from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country

❁ In the absence of an adequacy decision or appropriate safeguards, transfers shall take place only in following circumstances:

- a) **Consent** — based on individual's informed consent on specific cross-border data transfer.
- b) **Contract** — based on a contract between the individual and the organization.
- c) **Contract** - concluded in the interest of the data subject
- d) **Public interest** — important reasons of public interest.
- e) **Legal claims** — to exercise or defence of legal claims.
- f) **Vital interests** — vital interests of the individual or other persons, where the individual is incapable of giving consent.
- g) **According to EU law** — intended to provide information to the public on legitimate interest.



EU Digital Agenda

1. Proposal for ePrivacy Regulations
2. Provisions for Transfers to UK post-Brexit
3. Data Transfers to the US in the light of Schrems I and Schrems II cases -> Proposal of a Trans-Atlantic Data Privacy Framework



Open Data and Re-use of Public Sector Information Directive



- ✿ The Open Data Directive (EU) 2019/1024 mandates the release of public sector data in free and open formats.
- ✿ The overall objective of the Directive is to continue the strengthening of the EU's data economy by increasing the amount of public sector data available for re-use, ensuring fair competition and easy access public sector information, and enhancing cross-border innovation based on data.
- ✿ The main principle of the Directive is that **government data should be open by default and design**.
- ✿ The provisions of the Directive include:
 - ✿ Release of non-personal data in open formats and to open standards.
 - ✿ Data to be available in real time and via APIs (where possible).
 - ✿ New rules on charging - free reuse becomes a principle.
 - ✿ Re-use of publicly funded research data.
 - ✿ List of High Value Datasets (HVDs) to be laid down in an Implementing Act.
 - ✿ Prevention of data lock-in, exclusive arrangements discouraged.
 - ✿ Re-use of data held by public undertakings such as public utilities and transport providers.

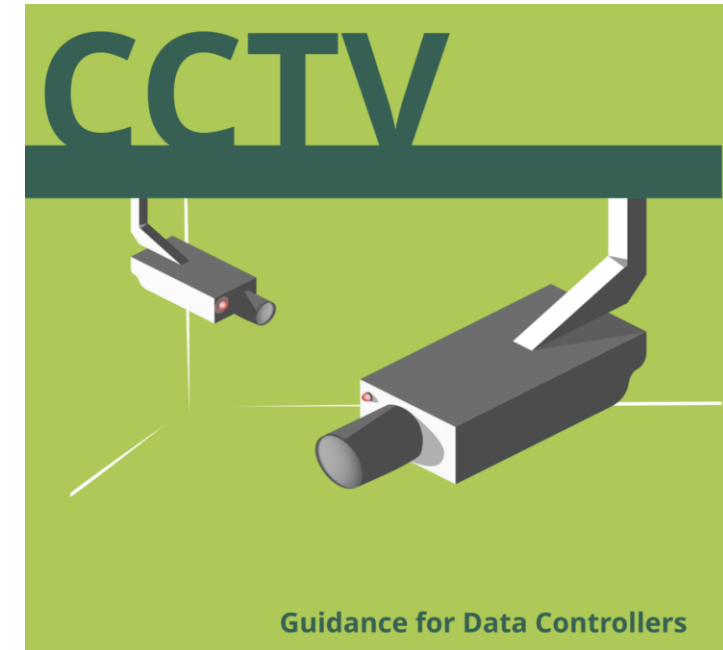
Privacy and Data Protection (Part III)

Data Protection in Practice



Surveillance

- ❖ CCTV systems must be used only where there is a **legitimate use** that is documented. **Data controllers must be aware of DP implications both ethical and legal**
- ❖ The **legitimate uses** could be for example in securing premises, supporting workplace safety management, and aiding in the prevention and detection of crime.
- ❖ Data controllers should be aware that **footage or images containing identifiable individuals captured by CCTV systems are personal data** for the purposes of data protection law.
- ❖ **Even** where processes are used to **obscure or de-identify** individuals from CCTV footage, the footage or images are still considered personal data **if it is possible to re-identify** the individuals (analogous to pseudo-anonymization)



CCTV Checklist

✖ Purpose

✖ Lawfulness

✖ Necessity

✖ Proportionality

✖ Security

✖ Retention

✖ Transparency

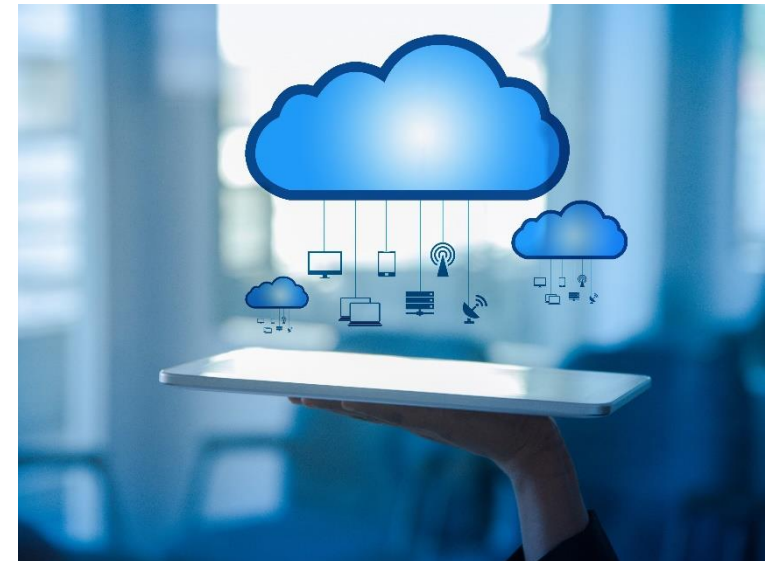
- Do you have a clearly defined purpose for installing CCTV?
- What are you trying to observe taking place?
- ...



Cloud Computing



- More and more enterprises are moving to the cloud
- Moving to the cloud applies a fundamental shift and how organisations collect, process, and share data
 - (1) general privacy and security challenges of cloud computing
 - (2) more GDPR specific challenges
- Organisations need to ensure there is adequate security for the personal data they process.



**Guidance for Organisations
Engaging Cloud Service
Providers**



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Security in Cloud Computing

The cloud service provider (CSP) should give assurances on key issues such as:

- ✿ pseudonymisation and encryption;
- ✿ isolation or separation of a personal data from the CSP's other customer data;
- ✿ ensure ongoing confidentiality, integrity, availability and resilience;
- ✿ restoration of availability and access in the event of a physical or technical incident;
- ✿ regular testing, assessing and evaluating the effectiveness of measures;
- ✿ procedures in the event of a data breach; and
- ✿ process to delete or return all personal data on contract termination.



Mechanisms of verification:

- ✿ requesting a detailed technical analysis incorporating an information security audit questionnaire or an approved code of conduct/certification mechanism
- ✿ on-site inspections of the CSP, implementation of the security policy and/or audit of personal data processing operations/technology usage

Auditing

🌐 Data controllers need to regularly audit their holdings of personal data and the procedures they have in place to protect this data.

Questions they should ask include:

1. Do we know what types of personal data we hold:
 - electronically (including less obvious data such as CCTV images)?
 - on paper?
2. Are we satisfied with the level of security (access, editing, deletion) on our own systems and its documentation
3. If we outsource processing of personal data to a data processor (including a 'cloud computing' service provider), are we satisfied that their security procedures are adequate?



Data Anonymization

Anonymisation



Example: Location data combined with



Example: Location data combined with a permanent ID



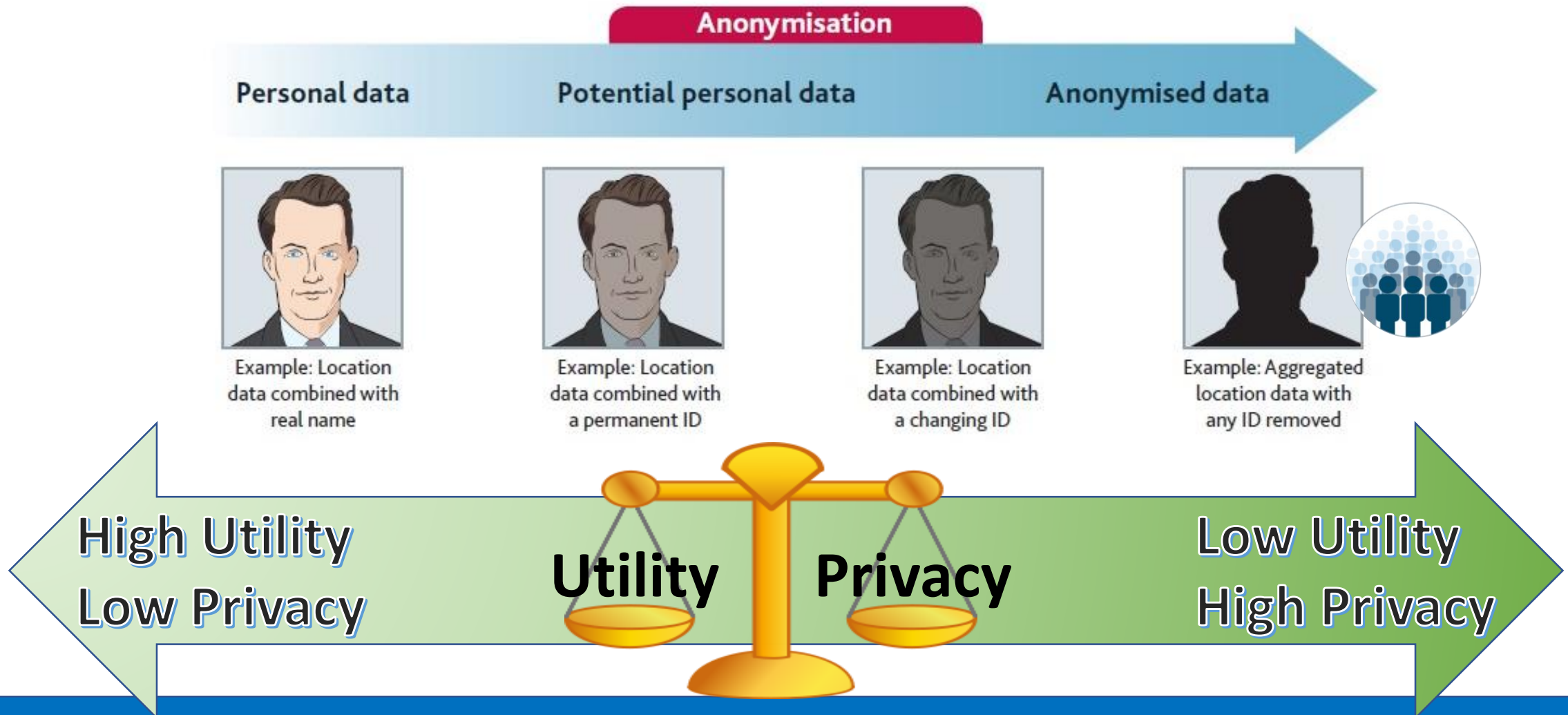
Example: Location data combined with a changing ID



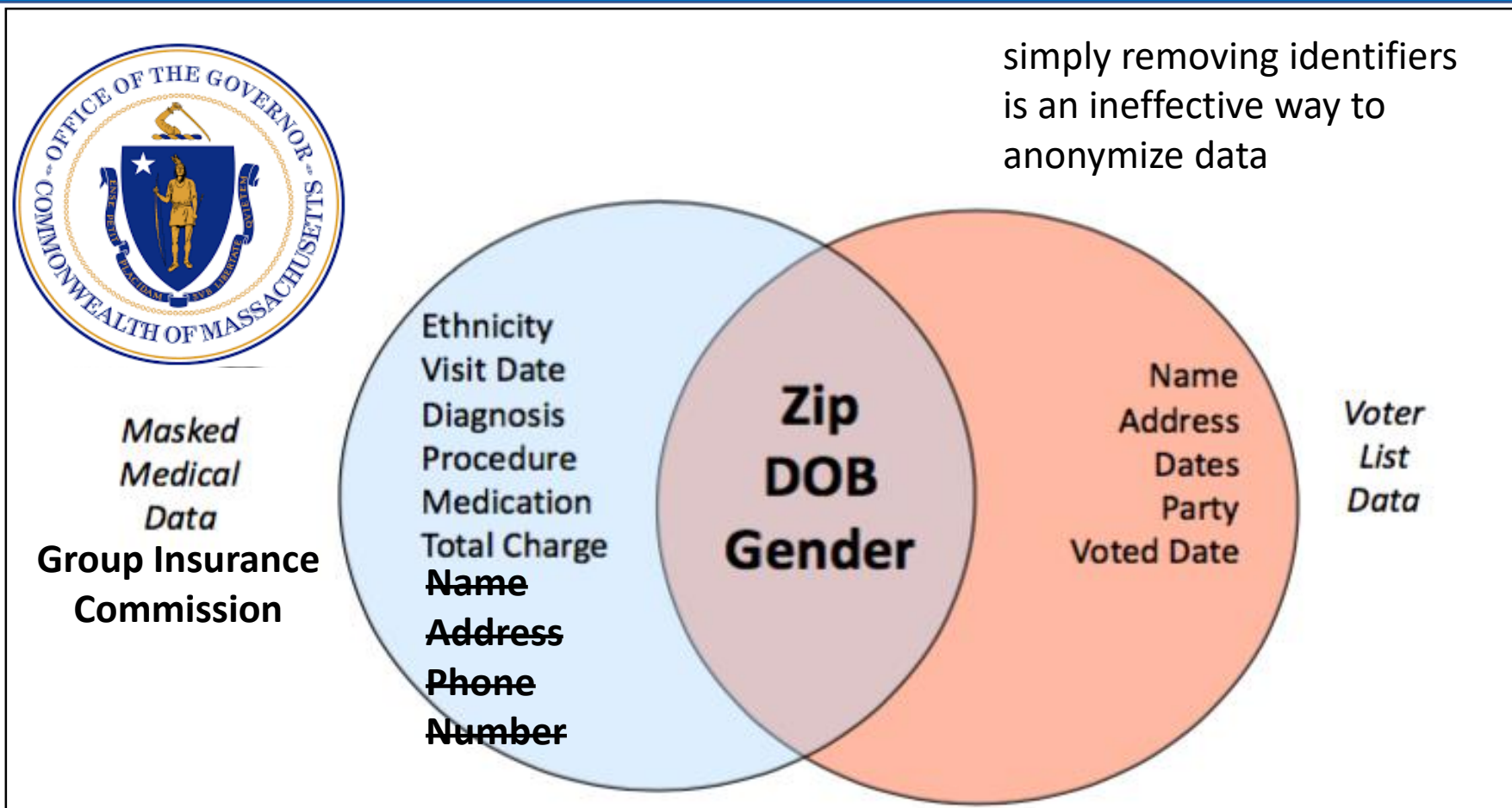
Example: Aggregated location data with any ID removed



Data Anonymization



Poor Anonymization



2002: Former Massachusetts governor's medical record re-identified

Poor Anonymization

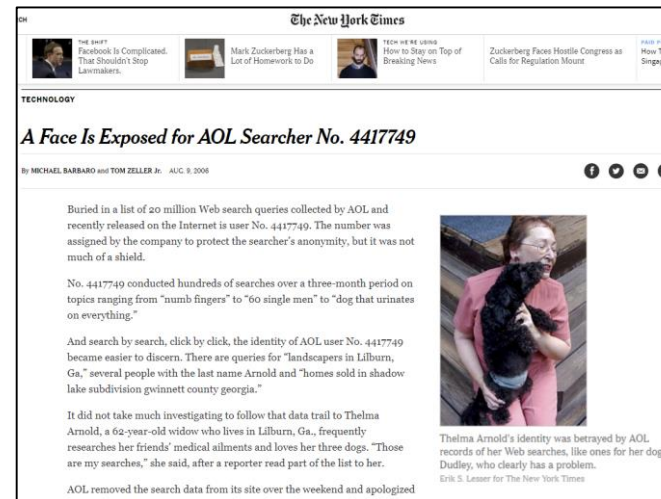
Cont.



2005: teenager tracked down his anonymous sperm donor father



2013: identity of anonymous DNA donors revealed



2006: Identity discovered: Thelma Arnold, a 62-years-old widow who lives in Lilburn, Georgia



2008: Subscribers identified

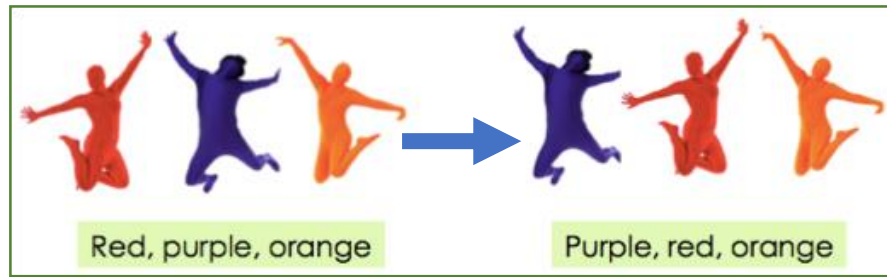


2014: NYC cab drivers' detailed whereabouts revealed

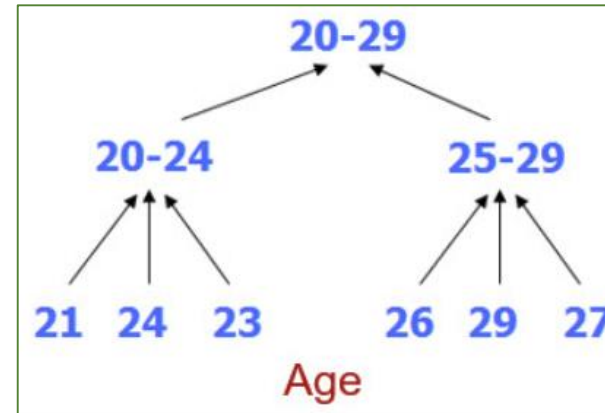
Anonymization Techniques



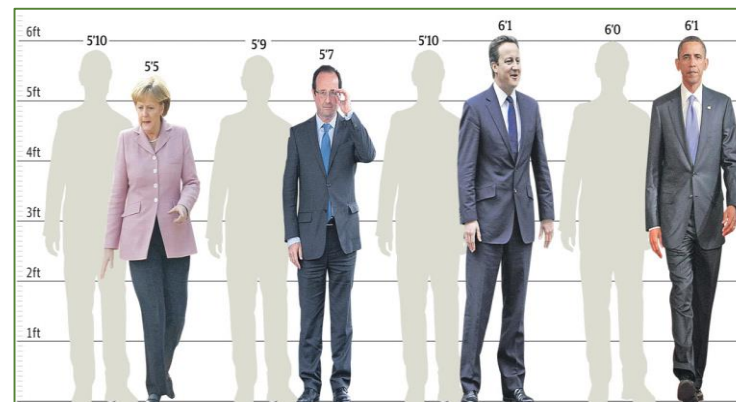
K-anonymity



Permutation



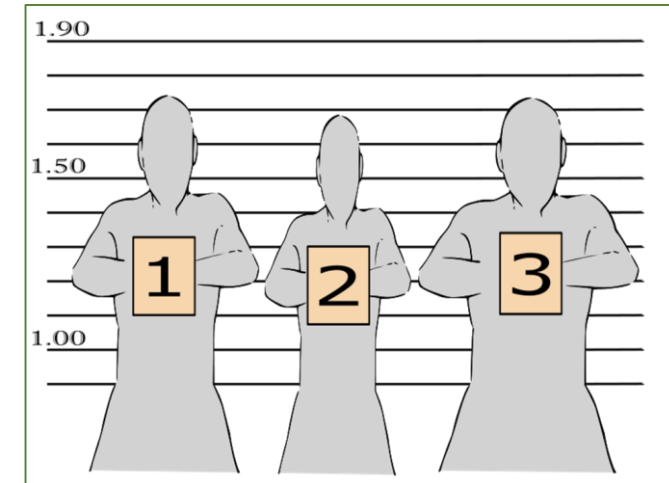
Generalization



Noise Addition

73301 – 73***
32003 – 32***
99501 – 99***

Truncation



Pseudonymization

Exercises

Suggestions for Exercises/Tutorials for Students



How to Get Students Involved



Presentations and discussion of case studies/landmark cases in legal instruments



Quizzes (Quizizz, Kahoot!) for retaining concepts and definitions



Critical review and group discussion of academic or industry papers



Practical exercises and tools for conducting DPIAs, Data Anonymization, etc.

Quiz on GDPR (5 Questions)

https://quizizz.com/admin/quiz/631b1b89f0b6e0001d621a59?source=quiz_share

Case Study 1:

Use of CCTV in the Workplace 1/3



Complain: DPC received a complaint that concerned **the use of CCTV cameras** by the data controller **in the complainant's work premises**, and **the viewing of that CCTV footage** (which contained personal data of the complainant, consisting of, among other things, images of the complainant) **for the purpose of monitoring the complainant's performance in the course of his employment** with the data controller.

Scenario: At the time of the complaint, the data controller had a CCTV **policy** in place, which **stated that the reason for the CCTV system was for security and safety**. This was also stated on signage in place in areas where the CCTV cameras were in operation. The facts indicated that the purposes for which the complainant's personal data was initially collected were security and safety. **However**, during a meeting with the complainant, a manager informed the complainant that CCTV footage containing the **complainant's personal data had been reviewed solely for the purposes of monitoring the complainant's performance in the course of the complainant's employment** with the data controller.

Moreover, in written responses to the DPC, the controller stated that, at the time of the complaint, **access to CCTV footage was available on a standalone PC in the department, which did not require log-in information**. The responses from the controller indicated that **access to CCTV footage was not logged either manually or automatically**.

Questions:

- What do you think is the legal basis used by the employer to use CCTV to monitor the workplace?
- What issues do you identify in the above scenario w.r.t. GDPR compliance?
- If there are any GDPR infringements, how they can be addressed?

Case Study 1:

Use of CCTV in the Workplace 2/3



Questions:

- ✿ What do you think is the legal basis used by the employer to use CCTV to monitor the workplace? **Legitimate Interest**
- ✿ What issues do you identify in the above scenario w.r.t. GDPR compliance?
 1. Further processing data which is incompatible with the original purpose GDPR Art 5(1)(b) Principles relating to processing of personal data -> Purpose Limitation)
 2. Process personal data fairly (GDPR Art. 5(1)(a)),
 3. The way the CCTV system and logs were accessed. (Art. 32 Security of processing)
- ✿ If there are any GDPR infringements, how they can be addressed?
 - ✿ CCTV policy must be substantially revised and replaced by a new policy
 - ✿ Access to CCTV recordings could be limited to a single individual in the specific unit and recordings are reviewed only in the event of a security incident or accident.

Complain: DPC received a complaint that concerned the use of CCTV cameras by the data controller in the complainant's work premises, and the viewing of that CCTV footage (which contained personal data of the complainant, consisting of, among other things, images of the complainant) for the purpose of monitoring the complainant's performance in the course of his employment with the data controller.

Scenario: At the time of the complaint, the data controller had a CCTV policy in place, which stated that the reason for the CCTV system was for security and safety. This was also stated on signage in place in areas where the CCTV cameras were in operation. The facts indicated that the purposes for which the complainant's personal data was initially collected were security and safety. However, during a meeting with the complainant, a manager informed the complainant that CCTV footage containing the complainant's personal data had been reviewed solely for the purposes of monitoring the complainant's performance in the course of the complainant's employment with the data controller.

Moreover, in written responses to the DPC, the controller stated that, at the time of the complaint, access to CCTV footage was available on a standalone PC in the department, which did not require log-in information. The responses from the controller indicated that access to CCTV footage was not logged either manually or automatically.

- ✿ What do you think is the legal basis used by the employer to use CCTV to monitor the workplace?
- ✿ What issues do you identify in the above scenario w.r.t. GDPR compliance?
- ✿ If there are any GDPR infringements, how they can be addressed?

Case Study 1:

Use of CCTV in the Workplace 3/3



DPC response:

- **Reviewing CCTV footage for the purposes of monitoring the complainant's performance** in the course of the complainant's employment with the data controller was **not one of the specified purposes of processing set out in the CCTV policy and signage**.
- The controller acknowledged that **the use of the complainant's personal data in this way was a contravention of its policies**.
- Where personal data is processed for a purpose that is different from the one for which it was collected, the **purposes underlying such further processing must not be incompatible with the original purposes**. In relation to the use of the complainant's personal data, **the purpose of monitoring their performance was separate and distinct from the original purposes** of security and safety for which the CCTV footage was collected. On that basis, the processing of the complainant's personal data contained in the CCTV footage for the purpose of monitoring performance was further processing for a purpose that was incompatible with the original purposes of its collection.
- **The absence of an access log for the CCTV footage was a deficiency in data security generally**. Data controllers must implement appropriate security and organisational measures, in line with Article 32 of the GDPR, in relation to conditions around access to personal data.
- **The CCTV policy has since been substantially revised and replaced by a new policy**. The controller confirmed that **the PC utilised has now been deactivated and removed**. Access to **CCTV recordings is now limited to a single individual** in the specific unit and **recordings are reviewed only in the event of a security incident or accident**.
- **Of particular relevance** in this type of situation are the obligations to process personal data fairly (Article 5(1)(a)), and to obtain such data for specific purposes and not further process it in a manner that is incompatible with those purposes (Article 5(1)(b)). Further, appropriate security measures should be in place to ensure the security of the personal data (Article 5(1)(f) and Article 32).

Data Anonymization

1/3

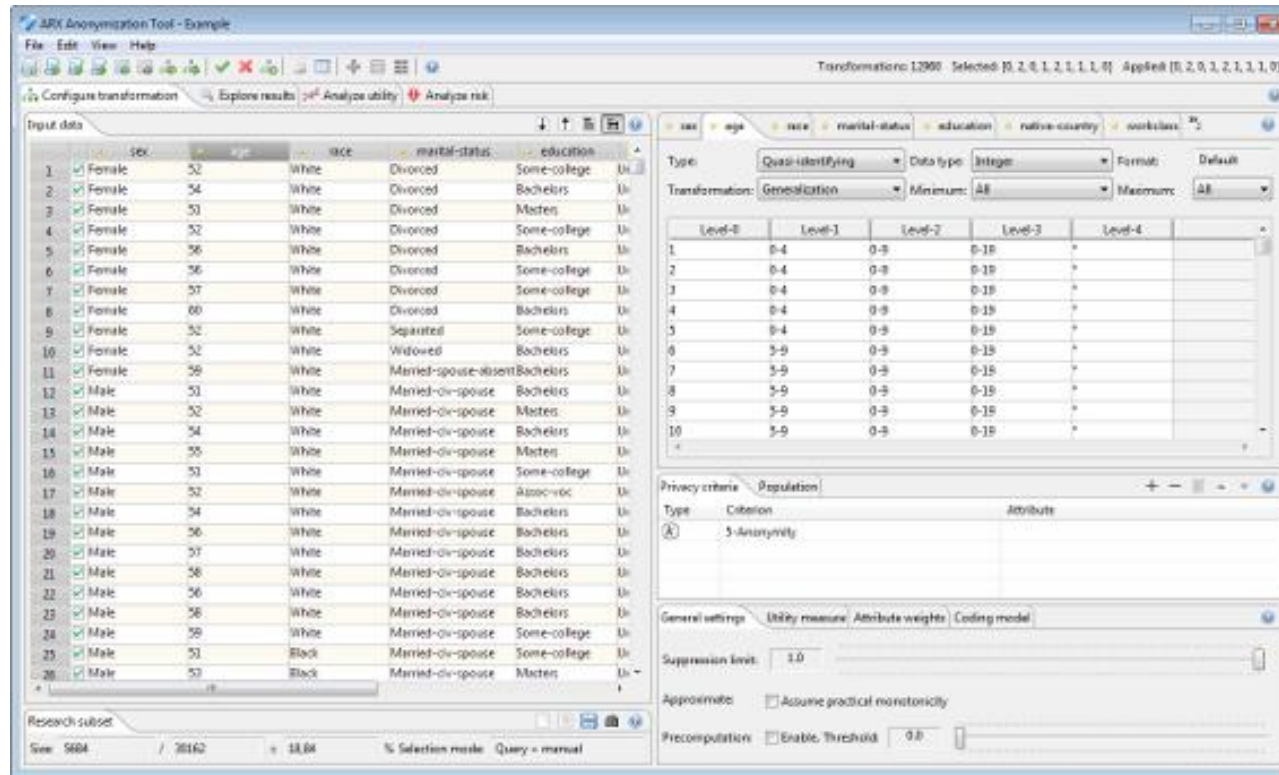


- **Tool:** ARX – Data Anonymization Tool
- **Website:** <https://arx.deidentifier.org/>



ARX – Data Anonymization Tool

A comprehensive software for privacy-preserving microdata publishing



Fabian Prasser*, Florian Kohlmayer*, Ronald Lautenschlaeger, Klaus A. Kuhn.

ARX – A Comprehensive Tool for Anonymizing Biomedical Data.

Proceedings of the AMIA 2014 Annual Symposium, November 2014, Washington D.C., USA. (Pubmed)

➤ **Go to:**

<https://arx.deidentifier.org/downloads/>

➤ **Download the ARX tool installer**

➤ **Download the example project**

➤ **Download additional datasets: irishcensus30m.csv**

<https://github.com/ucd-pel/COCOA>

➤ Elements in the Anonymization Process

- Dataset to anonymize
- Categorization of attributes (Identifiers, Quasi-identifiers, Sensitive Attributes)
- Generalization hierarchies for QIDs
- Anonymization algorithm
- Privacy level
- Search metric
- Data utility metric

Ayala-Rivera, Vanessa, Patrick McDonagh, Thomas Cerqueus, and Liam Murphy.
"A systematic comparison and evaluation of k-anonymization algorithms for practitioners."
Transactions on Data Privacy 7, no. 3 (2014): 337-370.

THANK YOU!



Follow us

