

Module: Data Governance, Compliance and Ethics

WEEKS 4-6: PRIVACY AND DATA PROTECTION (OVERVIEW)

TRAINRDM PROJECT

MAY 31ST, 2022

vanessa.ayala-rivera@ncirl.ie



This work is licensed under a [Creative Commons Attribution 4.0 International License \(CC BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)





Dr Vanessa Ayala-Rivera
vanessa.ayala-rivera@ncirl.ie

About Me

- Lecturer in the School of Computer Science at National College of Ireland / Researcher / Software Engineer
- PhD in Computer Science at University College Dublin, specialized in Data Security and Privacy
- Areas of interest: Software engineering, Information security, Privacy engineering, Regulatory compliance
 - Member of ACM, IEEE, IAPP
 - Scientific reviewer: TSE, TDP, IET Software Journal, SoSyM, RE, REFSQ, IEEE Consumer Electronics Magazine, CONISOFT

@vayalariv / 0000-0001-7449-6473

2.1.1 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.



2.1.2 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

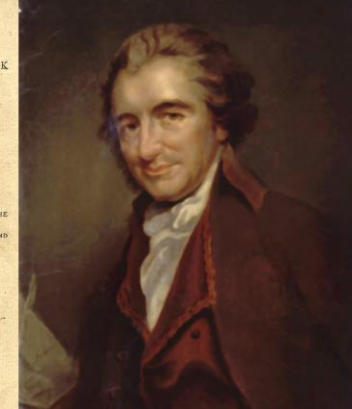
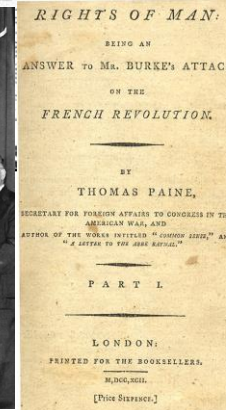
Privacy and Data Protection (Part I)

The right to privacy

- ✓ Brief History of Human Rights
- ✓ Privacy and confidentiality
- ✓ Types of EU legislation
- ✓ The Right to Privacy:
 - Constitution Of Ireland (1937)
 - Universal Declaration Of Human Rights (1948)
 - European Convention on Human Rights (ECHR, 1950)
 - The Charter of Fundamental Rights of the European Union (2000)



Guide on Article 8
of the European Convention
on Human Rights



“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 (owner of Purpose and Means)

- Comprehensive data protection laws are essential for protecting human rights
- 25th May 2022 – 4th 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

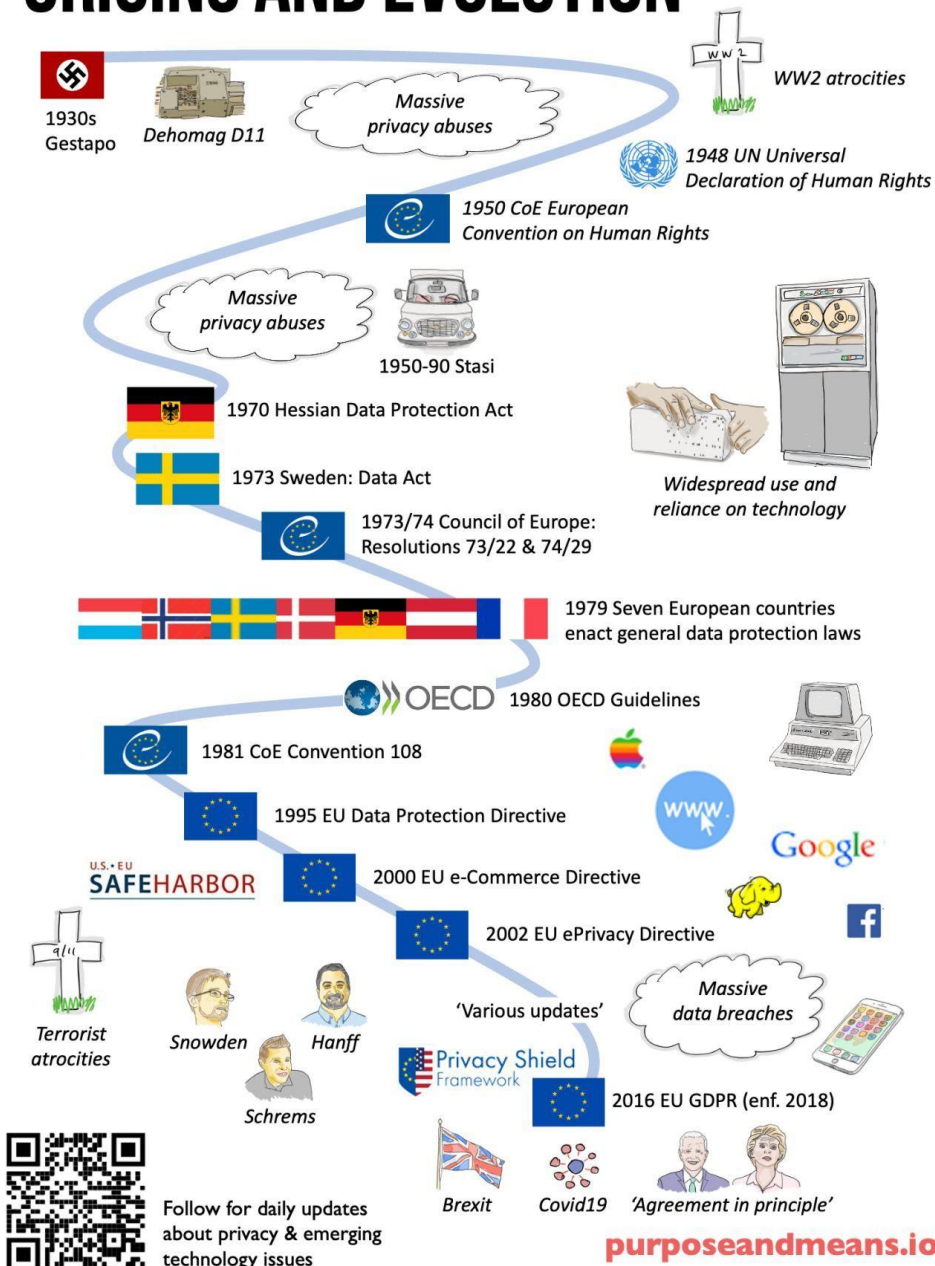


https://www.linkedin.com/posts/tim-clements-copenhagen_gdpr-privacy-dataprotecion-activity-6935111553465651200-n_xu

History and origins of European Data Protection legislation

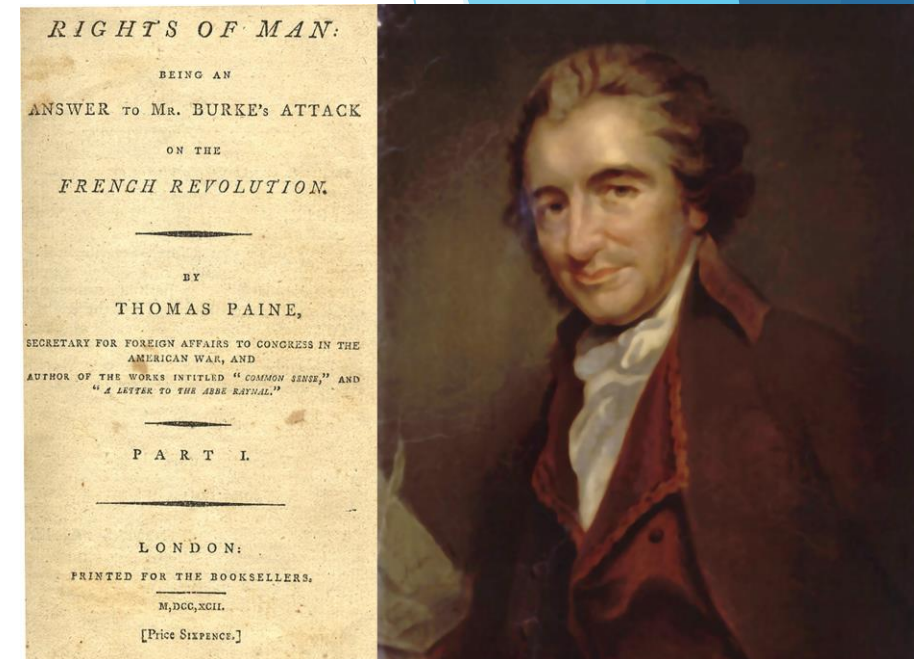
<https://www.youtube.com/watch?v=zVkaY6XeLEo>

EUROPEAN DATA PROTECTION ORIGINS AND EVOLUTION



A Short History of Human Rights

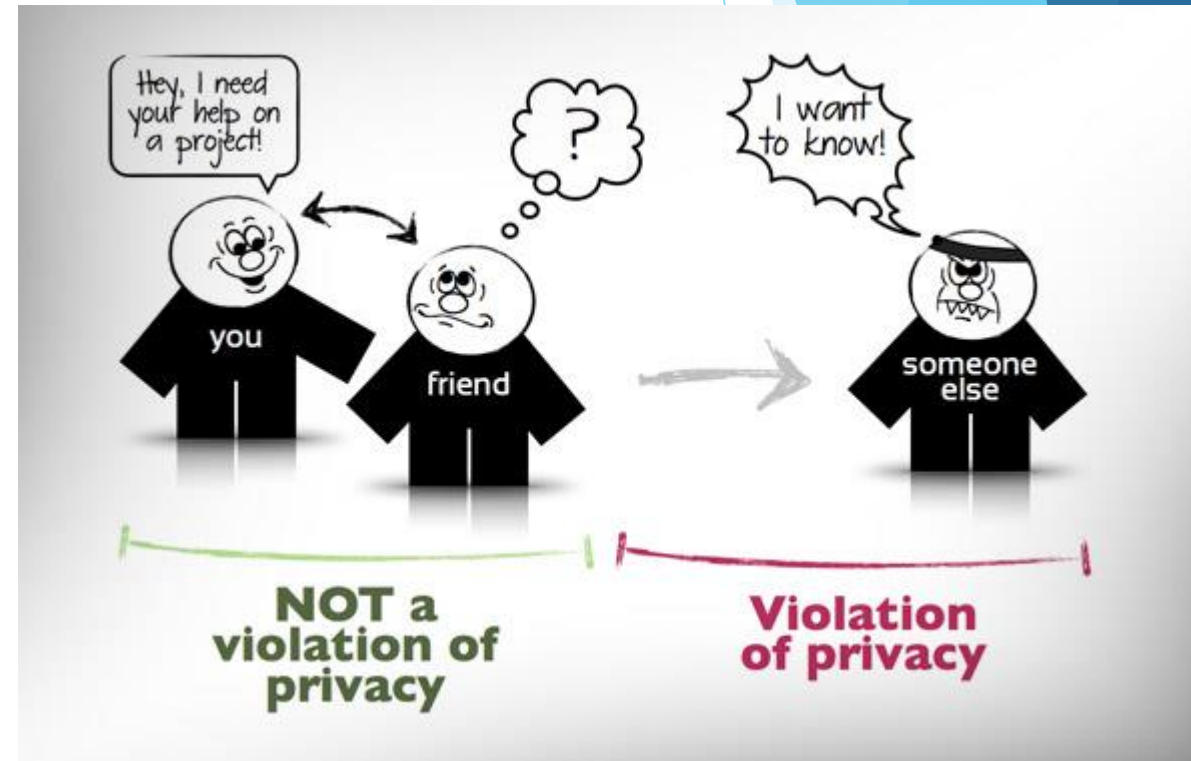
- ▶ Privacy underpins human dignity
- ▶ Universal human rights a relatively new concept but it does have its antecedents in documents through history:
 - Magna Carta (1215)
 - English Bill of Rights (1689)
 - French Declaration on the Rights of Man and Citizen (1789)
 - US Constitution and Bill of Rights (1791)
- ▶ Problem: Many of these excluded different groups and were therefore not universal.
- ▶ 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 in to its own).



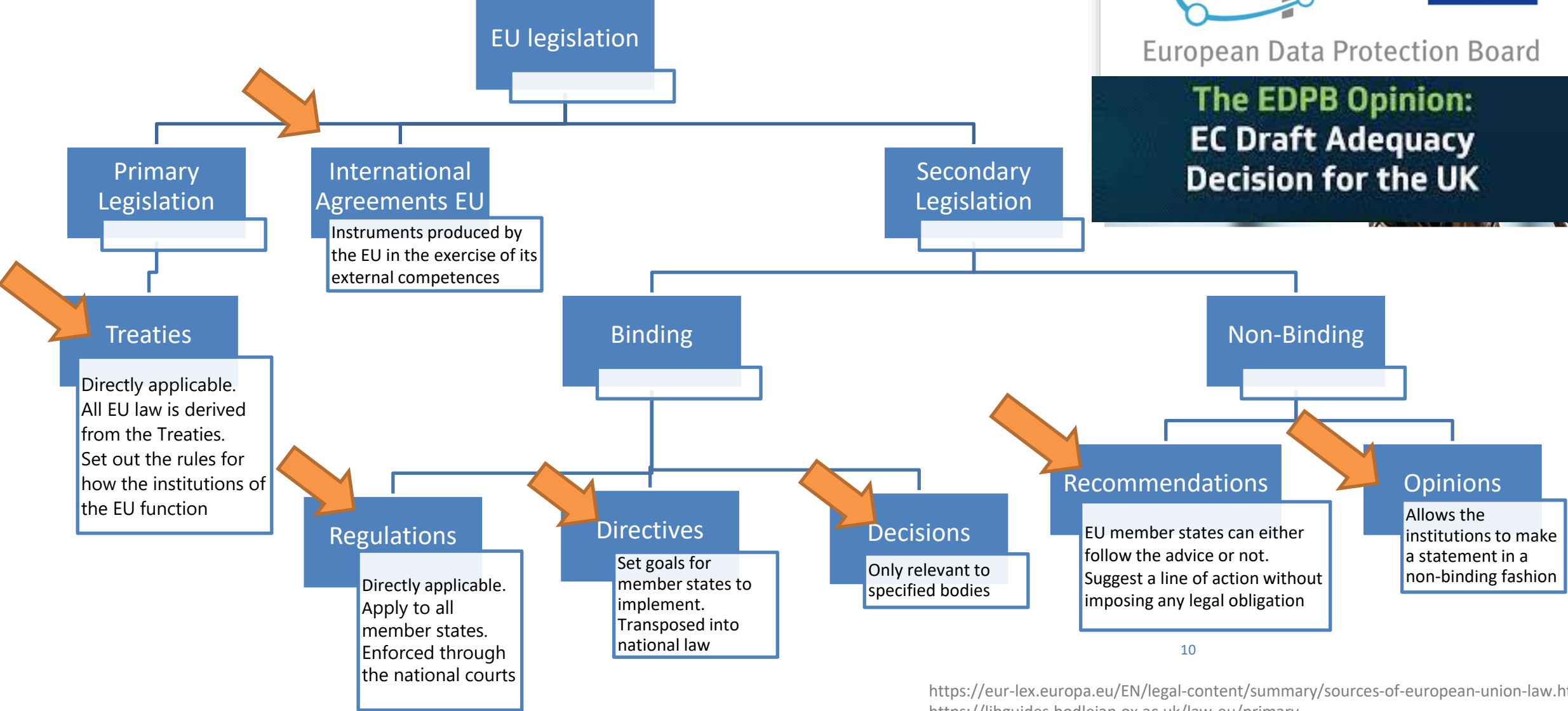
“popular political revolution is permissible when a government does not safeguard the natural rights of its people”

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



The Right to Privacy

The right to privacy in Ireland 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) enforced under the European Court of Human Rights
 - ✓ 1958: EU Charter of Fundamental Rights

The Right to Privacy

The right to privacy in Ireland 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) enforced under the European Court of Human Rights
 - ✓ 1958: EU Charter of Fundamental Rights

The Right to Privacy under Irish Constitution

- ❖ There are no direct references to privacy rights in the Irish Constitution
- ❖ The Right to Privacy has been recognised as one of the implied rights or so-called **unenumerated personal rights**, protected by Article 40.3.1 of the Constitution:

“The state guarantees in its laws to respect, and as far as practicable, by its laws to defend and vindicate the personal rights of the citizen.”

- ❖ Examples:
 - ✓ *McGee v Attorney General [1973]* : The right to marital privacy
 - ✓ *Kennedy and others v Ireland*: a breach of a journalist’s right to privacy

The Right to Privacy

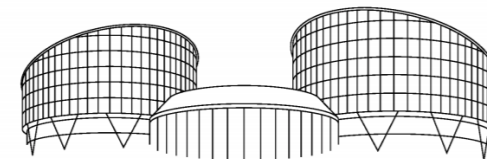
The right to privacy in Ireland is guaranteed both in:

1. The Constitution (National basic law)
2. European Level
 - ✓ 1948: UN Universal Declaration of Human Rights
 - ✓ 1953: European Convention on Human Rights (ECHR) enforced under the European Court of Human Rights (ECtHR)
 - ✓ 1958: EU Charter of Fundamental Rights

The Right to Privacy in the European Convention on Human Rights

1/2

- ▶ The Convention was based on the United Nations' Universal Declaration of Human Rights.
- ▶ Enforced in 1953 by the European Court of Human Rights (ECtHR)
- ▶ 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

https://www.echr.coe.int/documents/guide_art_8_eng.pdf

<https://www.coe.int/en/web/impact-convention-human-rights/right-to-privacy>

The Right to Privacy in the European Convention on Human Rights

Examples

2/2




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](#)

[READ MORE >](#)




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](#)

[READ MORE >](#)



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](#)

[READ MORE >](#)

European Court of Human Rights

- ▶ A.k.a. the Strasbourg Court, is an international court of the Council of Europe which interprets the European Convention on Human Rights
- ▶ The Convention established the European Court of Human Rights (ECtHR) in 1959 and is based in France
- ▶ The ECtHR oversees the implementation of the Convention in the 47 Council of Europe member states.
- ▶ Any person who feels their rights have been violated under the Convention by a state party can take a case to the Court.
- ▶ Judgments finding violations are binding on the States concerned and they are obliged to execute them.



Some Statistics :1959-2019

- ▶ Total Violations of the ECHE: 22,535
- ▶ Under Art 8 (Right to respect for privacy and family life): 1,475 (6.5%)
- ▶ Countries with most cases under Article 8:
 - Russian Federation: 220
 - Turkey 123
 - Poland 116
 - Italy 170
 - Romania 96

Ireland had 5 cases under the article



European Court of Human Rights, Strasbourg (image: wikipedia)

The Right to Privacy

The right to privacy in Ireland 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) enforced under the European Court of Human Rights (ECtHR)
 - ✓ 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.
- ▶ The Charter was declared in 2000, and came into force in December **2009** along with the Treaty of Lisbon.
- ▶ The Charter is **interpreted by the Court of Justice of the European Union (CJEU)**.

•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.



How is the Charter different from the European Convention on Human Rights?

- The Charter can be seen as the overarching framework for human rights in the EU, of which the European Convention on Human Rights forms only one part
- **All of the ECHR rights are included in the Charter.**
- **The Charter however addresses some modern issues** that are not included in the ECHR (for example, human cloning, data protection).

	European Convention on Human Rights (ECHR)	Charter of Fundamental Rights of the European Union
First (drafted by) proclaimed	1950 by the Council of Europe	2000 by the European Union
Came into effect in Ireland	European Convention of Human Rights Act 2003. Before this, the ECHR and the decisions of the European Court of Human Rights were not binding in Ireland but were referred to by the courts.	In December 2009 along with the Treaty of Lisbon. The Charter has the same legal status as an EU treaty and therefore has direct effect in certain areas.
When is it applied in Ireland?	Irish law must be compatible with the ECHR. This applies when laws are being written or changed and when the courts are interpreting Irish laws. Every government department, local authority and public institution must perform its duties in a way that satisfies Ireland's obligations under the ECHR.	The Oireachtas must consider the Charter when <i>transposing</i> EU directives into Irish law, or passing legislation following an EU decision or regulation. For citizens, the Charter only applies where the case involves EU law.
interpreted by Court	The European Court of Human Rights in Strasbourg	The Court of Justice of the European Union in Luxembourg

Implementation of the Charter

Rights provisions can be enforced through decisions in national courts or ultimately European Court of Justice

Fundamental rights agency provides for database of relevant court cases.

Under Article 8, some cases listed for Ireland

- ▶ Sony Music Entertainment Ireland Ltd & Ors v UPC Communications Ireland Ltd (28/07/2016)
- ▶ CRH PLC v The Competition and Consumer Protection Commission (04/05/2016)
- ▶ Recorded Artists Actors Performers Ltd v Phonographic Performance (Ireland) Ltd and Other (2020)

Ireland / High Court / [2014] IEHC 310

Subtitle: Maximilian Schrems v Data Protection Commissioner

Deciding body type: National Court/Tribunal

Deciding body: High Court

Type: Decision

Decision date: 18/06/2014

Policy area: Information society

CJEU Case C-311/13 / Judgment

Subtitle: Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems

Deciding body type: Court of Justice of the European Union

Deciding body: Court (Grand Chamber)

ECLI (European case law identifier): ECLI:EU:C:2020:559

Type: Decision

Decision date: 16/07/2020

Policy area: Information society

Implementation of Charter

Ireland / High Court / [2014] IEHC 310

Key facts of the case:

Edward Snowden, who worked for the US National Security Agency (NSA), unlawfully appropriated thousands of highly classified NSA files in 2013. He subsequently disclosed them to various media outlets and revealed the interception and surveillance of internet and telecommunications systems by the NSA on a global scale. The applicant claimed that Snowden's disclosures demonstrated that there was no effective data protection regime in the US and that the Irish Data Protection Commissioner should have exercised his statutory powers to direct that the transfer of personal data from Facebook Ireland to its parent company in the US should cease. The Commissioner maintained that he was bound by the terms of a Decision of the European Commission issued in 2000 to hold that the data protection regime in the US was adequate and effective where the companies which transfer or process the data to the US self-clarify that they complied with the principles set down in this Decision. This case was a judicial review of the Commissioner's decision where the Court questioned whether the proper interpretation of pre-Lisbon EU instruments should have been re-evaluated by the Commissioner in light of the subsequent entry into force of the Charter of Fundamental Rights.

CJEU Case C-311/13 / Judgment

5. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid.

Privacy and Data Protection (Part II)

- ✓ National law
- ✓ Data Protection Regulation Scope
- ✓ Data Controller & Data Processor
- ✓ Data Protection Principles
- ✓ Data Subject Rights
- ✓ Legitimate bases for processing
- ✓ Informed Consent



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

When Does the
GDPR Not Apply?



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



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



GDPR Exemptions

- ▶ In some instances, 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, which has been transposed into Irish law by way of the DPA 2018

EXEMPT

GDPR Loading

May, 25 2018



Scope of the GDPR

Article 2

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?



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 detecting motion.

Dr Mary Fairhurst said she had to move out of her home because of the doorbell installed by neighbour Jon Woodard.

Mr Woodward 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 that:

- 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 Fairhurst 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



Material Scope of the GDPR - DPC Ireland

I have a video doorbell that I can monitor on my smartphone – does that make me a data controller?

Similar to the cameras inside the home, a smart doorbell is likely to fall within the domestic exemption as its use will be connected purely with the homeowner's personal or household activity.

Where this may differ from the previous scenario is if the camera on the doorbell is pointed towards a publicly accessible area and is capable of recording individuals in that area.

The Court of Justice of the European Union has established in the case of 'Ryneš' that the use of a domestic CCTV system that covers a public space falls within the scope of data protection law.

To avoid this, when installing a smart doorbell care should be taken to avoid taking in a publicly accessible area. If this can't be avoided, a user should [consult our guidance on CCTV systems](#) to understand their transparency obligations.

Similarly, [the definition of 'personal data'](#) only covers information (in this case a video recording) where people are identified or identifiable.

What this means is any video footage which captures images of people where they can't actually be identified wouldn't be personal data at all. For example, the doorbell would probably capture a pretty clear picture of the person at the door, but might be designed or positioned so that any images of people on a public street are too obscured or low-quality to actually identify them.



Data Protection Commission Ireland @DPCireland · May 21

Do you have CCTV cameras outside your house pointing to your driveway and garden? Read our blog on CCTV in the home dataprotection.ie/en/cctv-home

Do you have CCTV cameras outside your house pointing to your driveway and garden?



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 with 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.



PERSONAL DATA

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

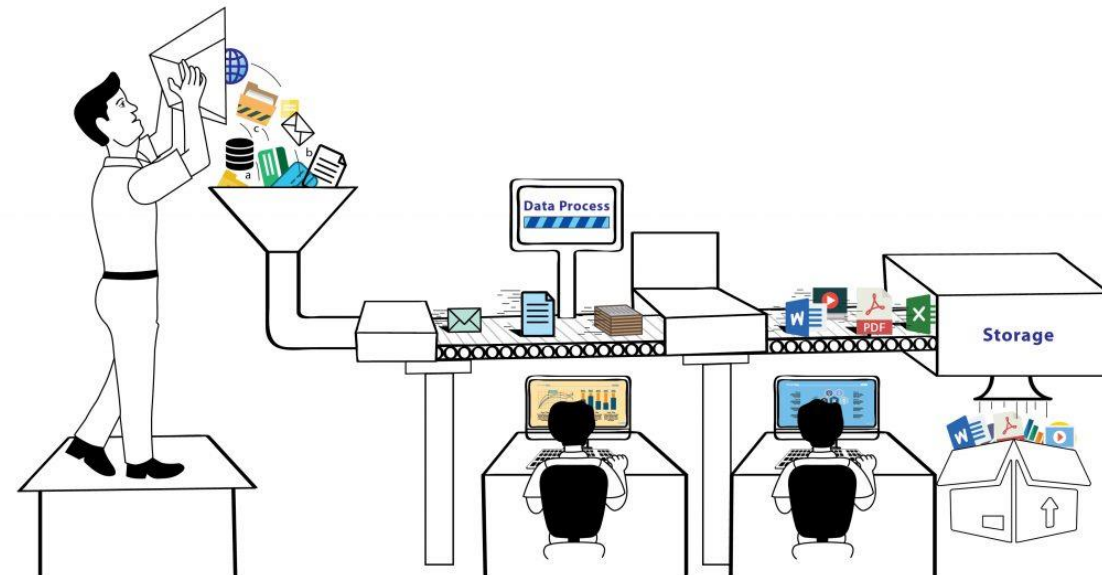
PERSONAL DATA	SPECIAL CATEGORIES	NOT PERSONAL DATA
<ul style="list-style-type: none">• name• email address (name.surname@domain.com)• phone number• Internet Protocol (IP) address• home address	<ul style="list-style-type: none">• criminal records• personal data related to racial or ethnic origin• medical records• religious or philosophical beliefs• trade-union membership• blood type• political stands...	<ul style="list-style-type: none">• a company registration number;• an email address as info@company.com• anonymized data• information about legal entities• data related to a deceased individual

PROCESSING

Art 4(2). 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.

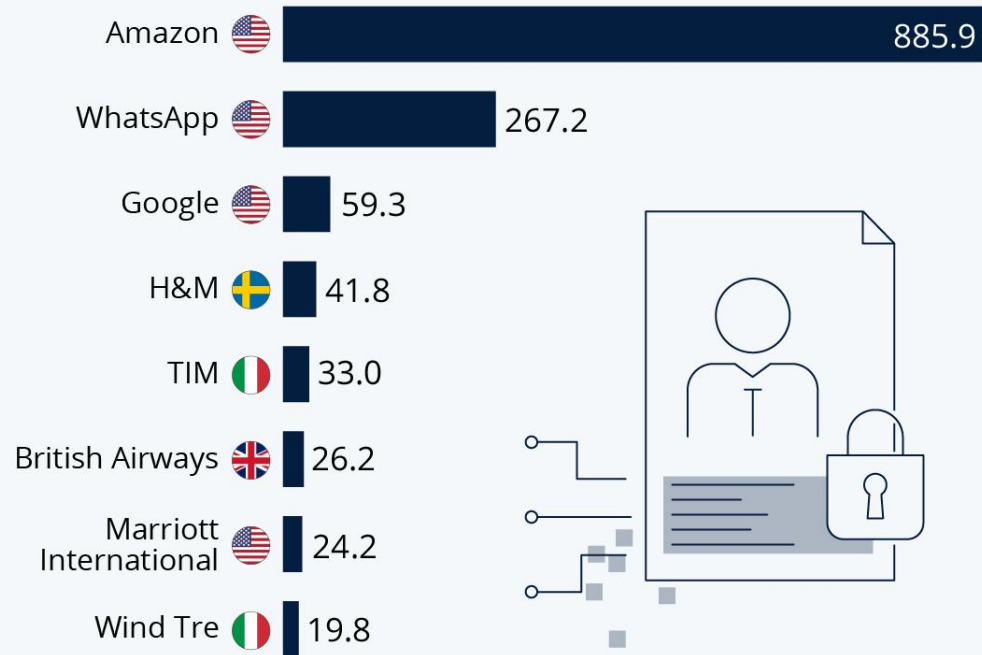


- Responsible for carrying out the actual processing
- Needs to maintain an audit trail of all processing activities

Administrative Fines

Big Tech, Big Fines

Highest fines for breaching one or more articles of the GDPR (in million U.S. dollars)



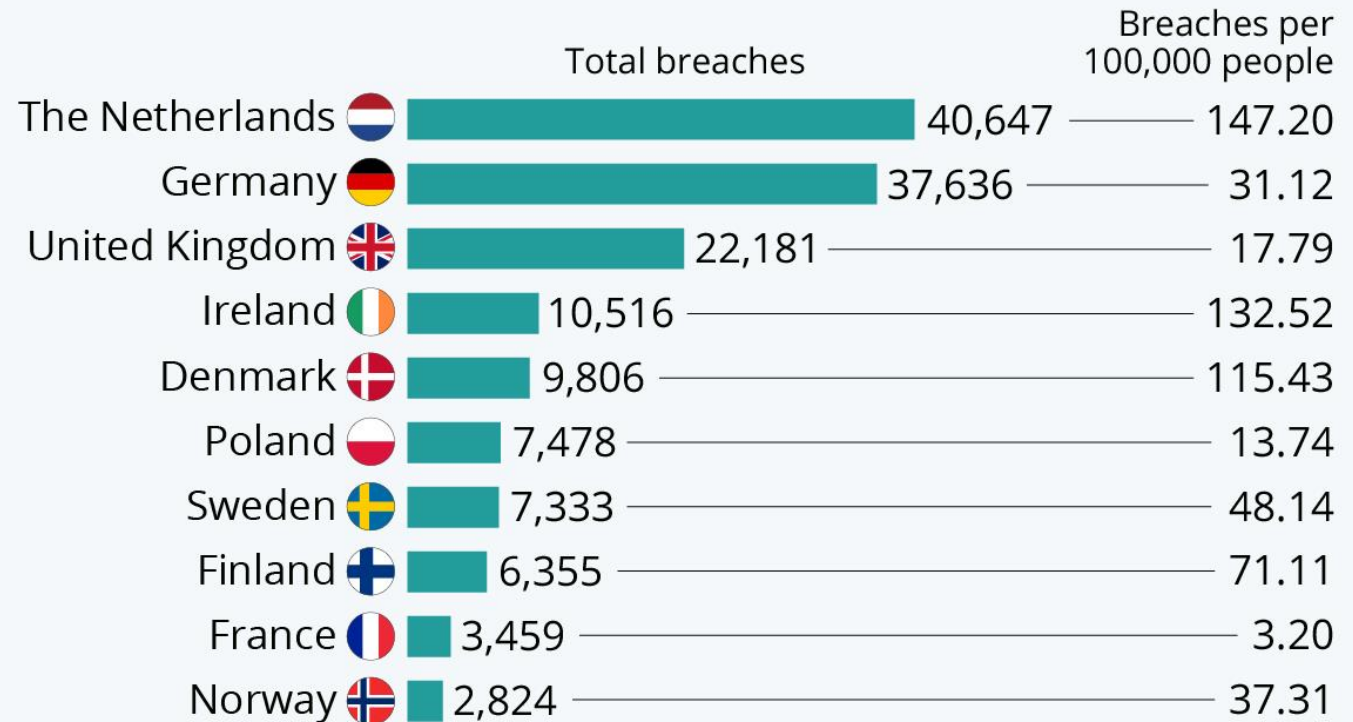
Source: CMS GDPR Enforcement Tracker



statista

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



statista

Case Study: Tusla - What It Cost Them?

- ▶ First in Ireland
- ▶ Organization disclosed children's information to unauthorized individuals on 3 different occasions.
- ▶ The decision found that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate measures with regard to the redaction of documents.
- ▶ Total fine: € 75.000
- ▶ In May 2020, Tusla received another fine of € 40.000 after it sent a letter containing allegations of abuse to a third party who then uploaded it to social media.



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)

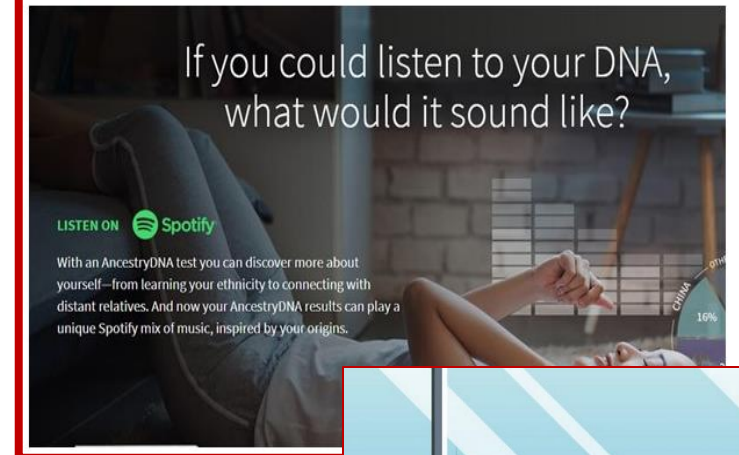
Principles Relating To Processing Of Personal Data

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



LAWFULNESS OF PROCESSING

GDPR Art. 6 Processing shall be lawful only if and to the extent that at least one of the following applies:



Informed consent and ethics

- ▶ Informed consent is the cornerstone of research ethics.
- ▶ Whenever you collect personal data directly from research participants, **you must seek** their informed consent by means of a procedure that **meets the minimum standards of the GDPR.**
- ▶ As with any research project involving human subjects, **if the data processing entails potential risks to the data subjects' rights and freedoms, they must be made aware of these risks during the informed consent procedure.**



CONDITIONS FOR CONSENT

GDPR Art. 7

- ▶ The controller must be able to prove consent
- ▶ Before consent is given, the data subject must be notified that they can withdraw consent
- ▶ If the consent is in writing, it must be clear, and no part may infringe on the GDPR
- ▶ The data subject can withdraw consent at any time, but this does not apply to anything processed while consent was active
- ▶ It determining if consent is given freely, issues such as contractual obligations or service conditions must be considered

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

RIGHTS OF THE DATA SUBJECT

Art. 12-23



*planio

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.

Privacy by Design and By Default (Art. 25)

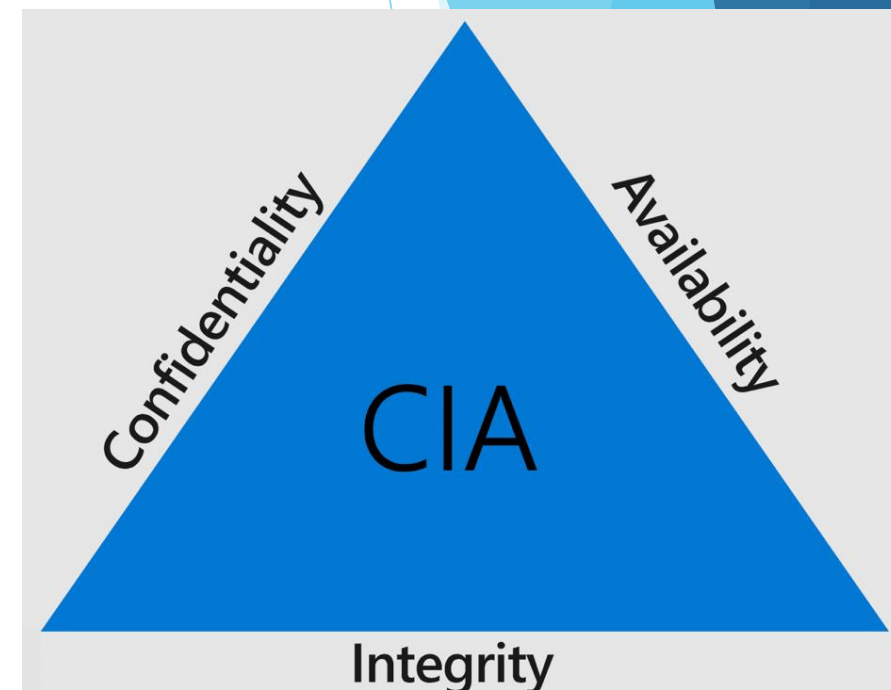
Ann Cavoukian, former Information and Privacy Commissioner of Ontario coined the Privacy by Design concept

- 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

SECURITY OF PROCESSING

GDPR Art. 32

- ▶ The pseudonymisation and encryption of personal data
- ▶ The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- ▶ The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- ▶ A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing



Open Data and re-use of Public Sector information Directive (EU) 2019/1024

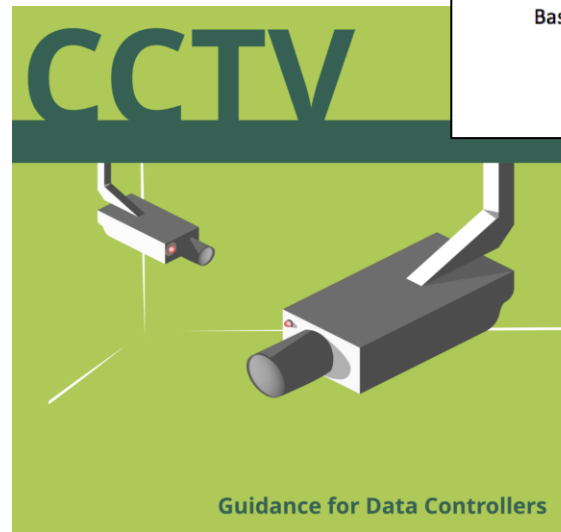
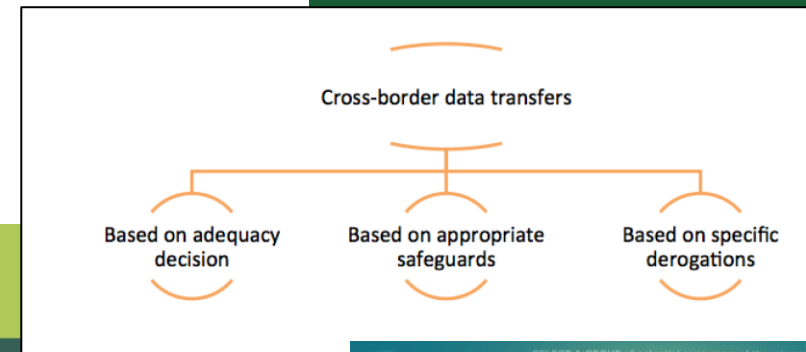
The Open Data Directive mandates the release of public sector data in free and open formats. The overall objective of the Directive is to continue the strengthening of the EU's data economy by increasing the amount of public sector data available for re-use, ensuring fair competition and easy access 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 publically 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
 - ✓ Data Transfers to Third Countries
 - ✓ Surveillance
 - ✓ Cloud computing
 - ✓ Auditing
 - ✓ Current Issues/Reforms



Data Protection in practice: international transfers to “third countries”

What happens when data transfers are required for international commerce or co-operation?

- ▶ EU law requires that this is done in a way that is “essentially equivalent” to those required under EU law (EDPB, 2000)
- ▶ 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.
- ▶ If transfers cannot be undertaken at the higher level (e.g., adequacy), then a lower level must be relied upon with correspondingly increased responsibility on data controllers to ensure that transfers are lawful

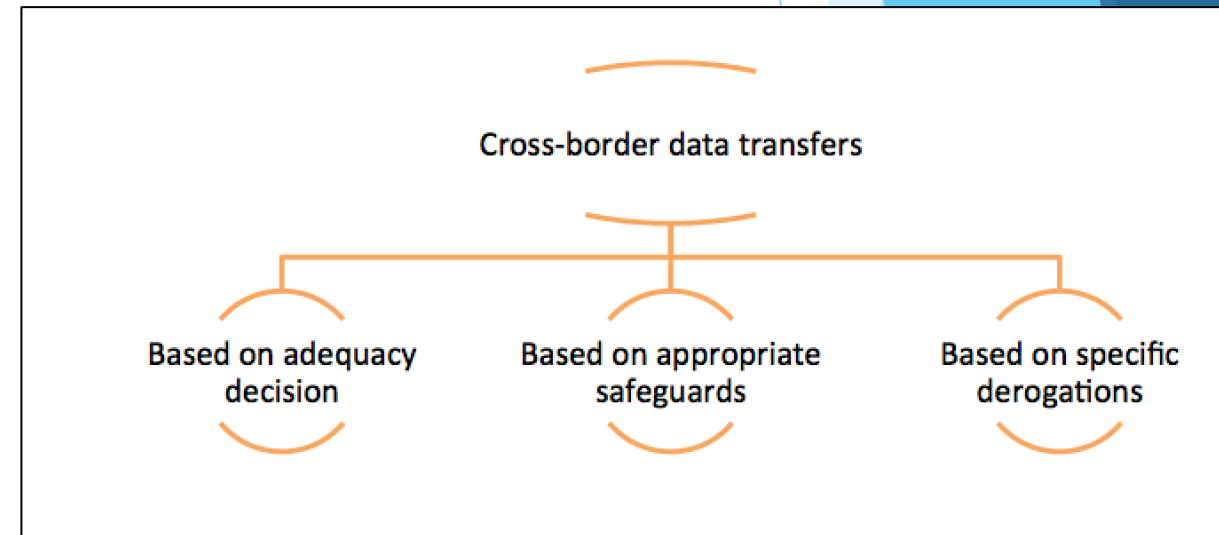
Chapter 5	
Transfers of personal data to third countries or international organisations	
Article 44	– General principle for transfers
Article 45	– Transfers on the basis of an adequacy decision
Article 46	– Transfers subject to appropriate safeguards
Article 47	– Binding corporate rules
Article 48	– Transfers or disclosures not authorised by Union law
Article 49	– Derogations for specific situations 47
Article 50	– International cooperation for the protection of personal data

A tiered approach

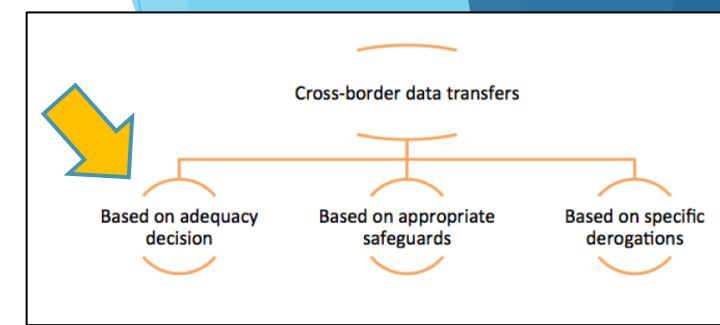
Data Protection in practice including international transfers



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 on the basis of an adequacy decision (Art. 45 GDPR)



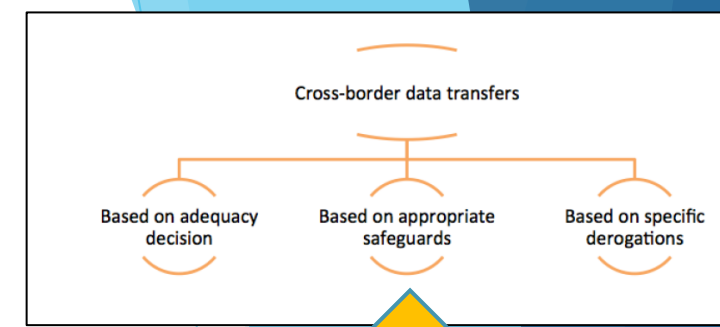
- ▶ 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level 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

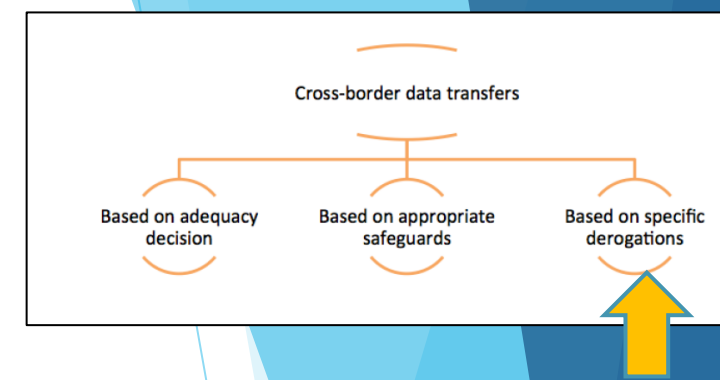
The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, the United Kingdom under the GDPR and the LED, and Uruguay as providing adequate protection. South Korea is in the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

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 Approved BCRs: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

Art.49 Transfers on the basis of specific derogations



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) the data subject has **explicitly consented** to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- (b) the transfer is necessary for the **performance of a contract** between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- (c) the transfer is necessary for the conclusion or performance **of a contract concluded in the interest of the data subject** between the controller and another natural or legal person;
- (d) the transfer is necessary for important reasons of **public interest**;
- (e) the transfer is necessary for the establishment, **exercise or defence of legal claims**;
- (f) the transfer is necessary in order to protect the **vital interests of the data subject or of other persons**, where the data subject is physically or legally incapable of giving consent;
- (g) the transfer is made from a register which according to Union or Member State law is intended **to provide information to the public** and which is open to consultation either by the public in general or by any person **who can demonstrate a legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Legal Bases For International Transfer Of Personal Data Under GDPR

Adequacy Decision

All EEA countries

Plus approved countries

Appropriate Safeguards

Standard Contract
Clauses (SCC)

Approved code of
conduct (CoC)

 Privacy Shield

Binding Corporate Rules (BCR)

Intra group
transfers only

Approved by the
Supervisory Authority

Exceptions ("Derogations")

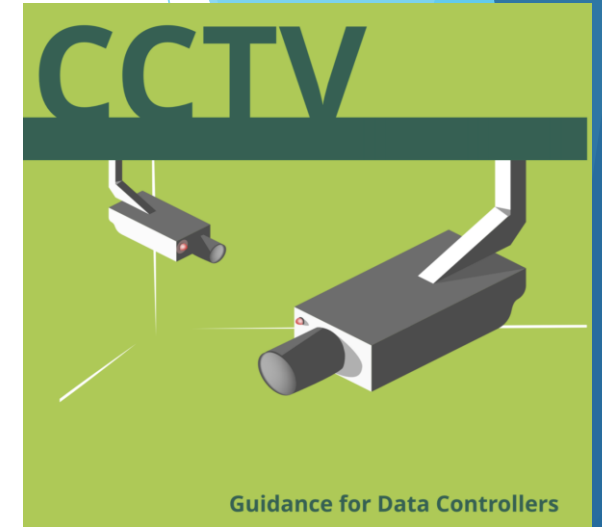
Consent of the
individual

Contractual obligation
for the individual

Vital interests of the
individual

Data Protection In Practice Including 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

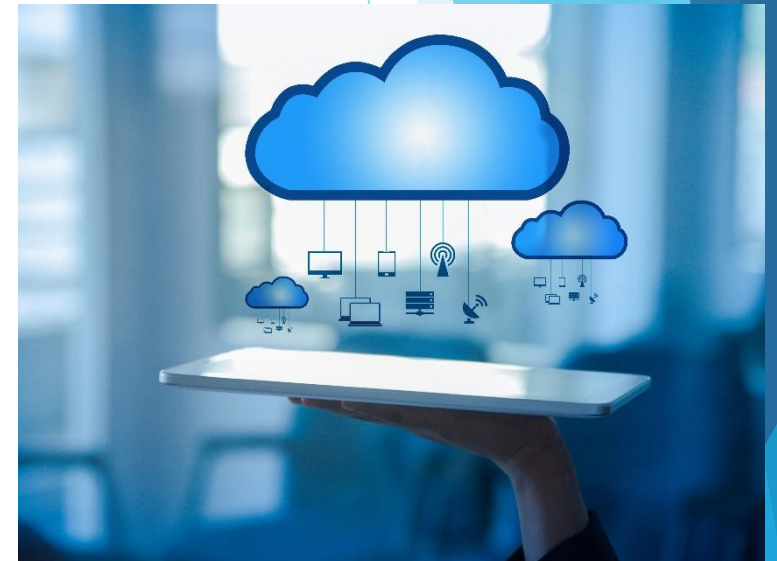
- ▶ Purpose
- ▶ Lawfulness
- ▶ Necessity
- ▶ Proportionality
- ▶ Security
- ▶ Retention
- ▶ Transparency

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



Data Protection in practice including cloud computing

- ▶ There are an increasing number of services offering ‘cloud storage’, allowing documents, photos, videos, and other files be uploaded to and stored on a remote server, to enable sharing or remote access, or to act as a backup copy.
- ▶ The use of any cloud services as part of their business is an important area in which 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 provider should be in a position to **give assurances on key issues** such as:
 - ▶ The **pseudonymisation** and **encryption** of personal data if required.
 - ▶ The **isolation or separation** of a personal data provided by the controller from the cloud provider's other customers' data.
 - ▶ The ability to **ensure the ongoing confidentiality, integrity, availability** and resilience of processing systems and services. This encompasses the **organisational and technical means**, from staff confidentiality requirements to meeting the security requirements of **Article 32 GDPR**.
 - ▶ The ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident.
 - ▶ A process for **regularly testing**, assessing and evaluating the effectiveness of technical and organisational **measures for ensuring the security of the processing**.
 - ▶ **Procedures in the event of a data breach**. This will practically mean that an incident response plan is in place and that a binding agreement on breach notification between the processor and controller is made, so that data subjects are not unnecessarily put at risk.
 - ▶ **A means to delete or return all personal data** to the controller when a contract terminates
 - ▶ Further aspects to consider: “7 Cloud Security Questions You Need to Ask Your Cloud Provider”

<https://solutionsreview.com/cloud-platforms/7-cloud-security-questions-you-need-to-ask-your-cloud-provider/>

Data Protection in practice including 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?



Audit questions

	Question	Controller	Processor
Personal data	Are you processing personal data?	✓	✓
Sensitive (special) personal data	Are you processing sensitive personal data?	✓	✓
Children's personal data	Is personal data of children collected and processed?	✓	✓

	Question	Controller	Processor
Lawful grounds for processing	Is there a lawful ground for processing the personal data for each processing operation?	✓	
	Is there a lawful ground for processing any sensitive personal data for each processing operation?	✓	
Consent	How is consent collected?	✓	
	How is this consent demonstrated?	✓	
	Can subjects withdraw their consent?	✓	

	Question	Controller	Processor
Notification of data subject	Is the data subject notified of processing?	✓	
Source of personal data and information provided to data subject	Is data collected direct from the subject and is the required information given to them?	✓	
	Is the data not collected from the subject and is the required information given to them?	✓	

	Question	Controller	Processor
Purpose limitation	Is personal data only used for the purposes for which it was originally collected?	✓	
Data minimisation	Is the personal data limited to what is necessary for the purposes for which it is processed?	✓	
Accuracy	Are policies and training in place to ensure personal data are checked and where inaccurate are rectified without delay?	✓	
Storage limitation (retention)	Do privacy policies incorporate information on retention? Are there procedures in place for archiving and destruction of data?	✓	
Integrity and confidentiality	Are appropriate security measures used to protect the data?	✓	
Accountability	Can you demonstrate compliance with the data protection principles?	✓	

	Question	Controller	Processor
	Are industry standard encryption algorithms and technologies employed for transferring, storing, and receiving individuals' sensitive personal information?	✓	✓
	Is personal information systematically destroyed, erased, or anonymised when it is no longer legally required to be retained or to fulfil the purpose(s) for which it was collected?	✓	✓
	Are steps taken to pseudonymise personal data where possible?	✓	✓
	Can the availability and access to personal data be restored in a timely manner in the event of a physical or	✓	✓

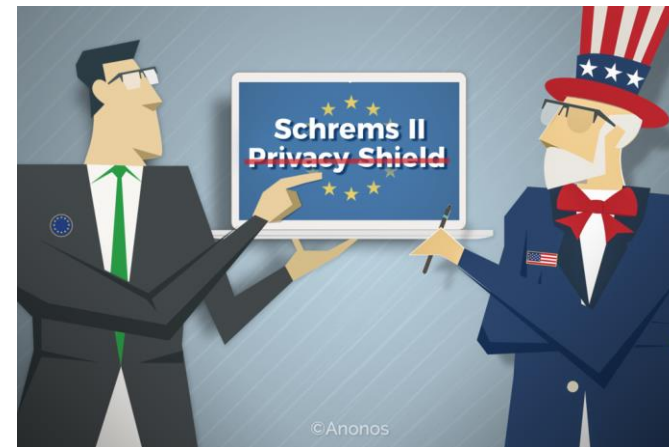
	Question	Controller	Processor
International data flow mapping	Is personal data transferred outside the EEA?	✓	✓
	What type of personal data is transferred and does this include any sensitive personal data?	✓	✓
	What is the purpose(s) of the transfer?	✓	✓
	Who is the transfer to?	✓	✓
	Are all transfers listed - including answers to the previous questions (e.g. the nature of the data, the purpose of the processing, from which country the data is exported and which country receives the data and who the recipient of the transfer is?)	✓	✓
	Is the legal transfer adequacy mechanism for each transfer identified and listed?	✓	✓



Current Issues/Reforms

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

The ePrivacy Regulation What to Expect



Any Comments
or Questions?

