KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

EU Data Protection Law: Fundamentals of the Legal Framework

Elora Fernandes

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Academy of European Law. Neither the European Union nor the granting authority can be held responsible for them.

Class overview

The development of EU data protection law

Key Concepts

The core data protection principles

The development of EU data protection law

In the 20th century, ideas on regulating personal data first emerged in:


United States


Japan


Germany


Sweden

Privacy

- “The Right to Privacy”- Samuel Warren and Louis Brandeis (1890)

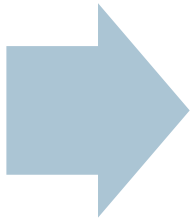
  = The right to be let alone

- Occurrences of popular resistance arose against the processing of data related to individuals in the 1950s (e.g., the census including questions on religious preferences), but the issue of "Computers and Privacy" began to be discussed in the U.S. only in the 1960s.
- Computer specialists started to raise concerns that computers process information quickly and inexpensively, while governmental agencies were collecting increasing amounts of data.

Informational Privacy

- Alan Westin's 1967 book "Privacy and Freedom" provided a new conceptualization of privacy in light of the technological advancements.
  - Privacy as the ability to exercise some control over the use of information about oneself.

Privacy as secrecy (freedom from intrusion)



Privacy as control of personal information

- 1970s – Fair Information Practice Principles

First wave of regulatory activities in Europe

- 1970 – German federal state of Hesse (*Hessische Datenschutzgesetz*)
- 1973 – Swedish Data Act
- 1977 – German Federal Data Protection Law
- 1978 – French Law on Computers, Files and Freedoms

Early Constitutional Recognition of data protection as a fundamental right:

- 1976 – Portugal
- 1978 – Austria
- 1978 – Spain

Important international developments

- 1980 – OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  - The world's first international statement of principles governing data processing;
  - Intended to balance privacy with the free flow of information.

- 1980 – Council of Europe (CoE)'s Convention 108
  - Driven by the need to align disparities in national laws.

EU Level

- 1995 – Data Protection Directive (DPD)
- Treaty of Lisbon (2009) and the new fundamental right to data protection (Article 8)

Article 8

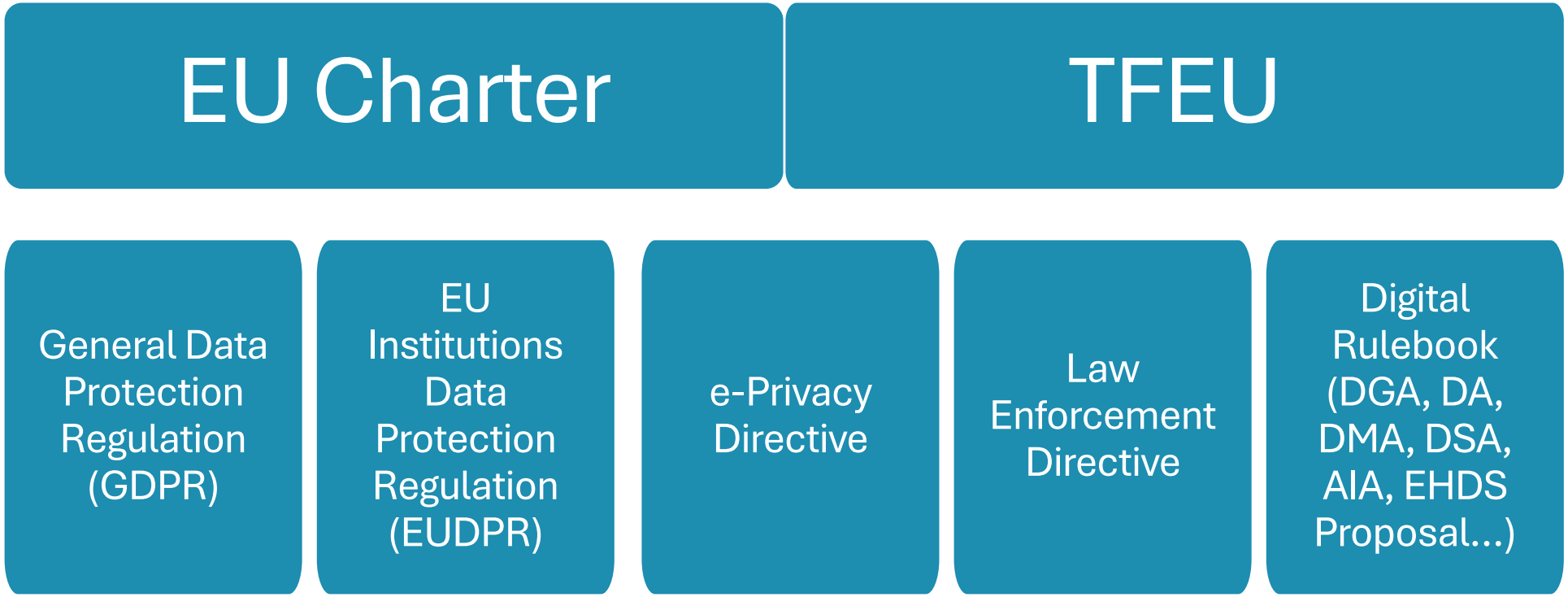
Protection of personal data

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.

Current sources of EU data protection law



Key concepts of the GDPR

Material Scope of the GDPR

Article 2

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.

Territorial Scope of the GDPR

Article 3

Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

What is personal data?

Article 4(1): ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Scenario 1 – Personal data

A video surveillance system is installed in a public square, recording video footage of the area. The footage captures people walking, sitting on benches, and engaging in daily activities. The video does not include any specific names or contact details, but faces and physical characteristics of individuals are clearly visible. The footage is stored by the system operators for security purposes. Can this footage be considered personal data under the GDPR?

What is processing?

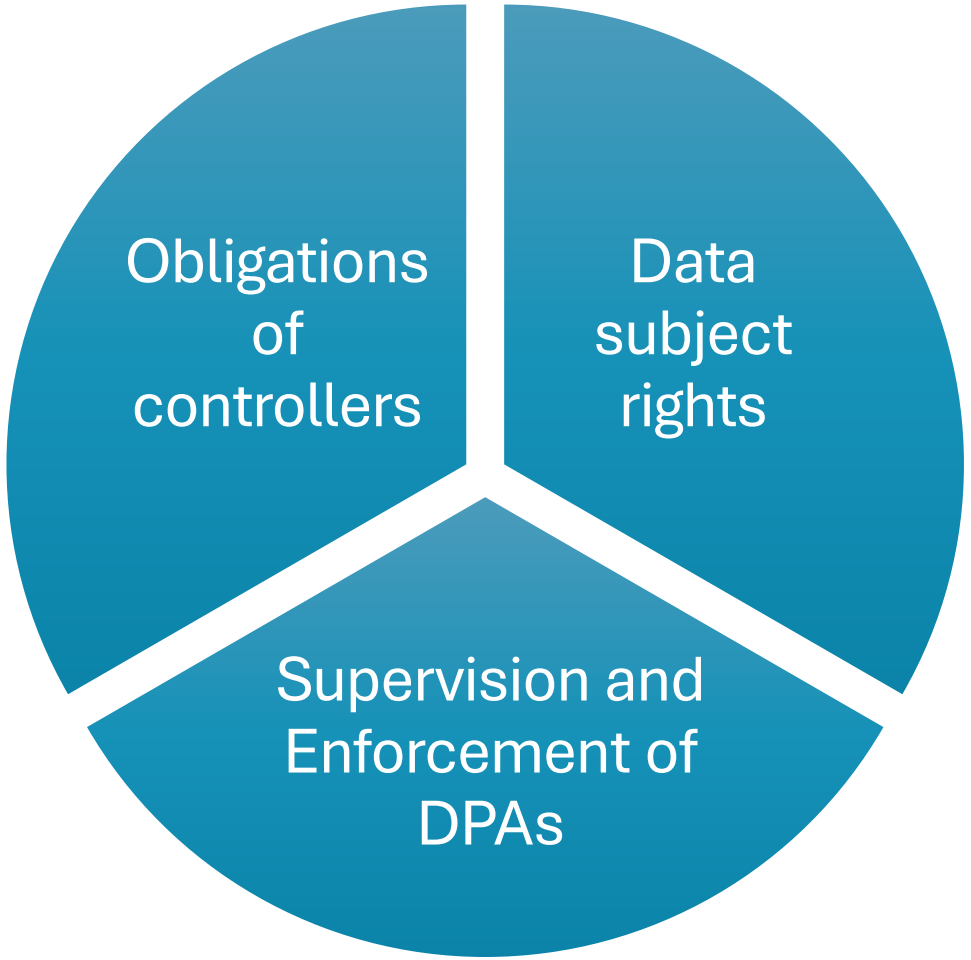
Article 4(2): ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Scenario 2 – Processing data

A company uses an automated software system that receives and stores email addresses entered by customers for a newsletter subscription. The system collects, stores, and organizes the email addresses but never sends any newsletters because the company halted its marketing efforts. Is the company still engaged in "data processing" under the GDPR?

Main “actors” of the GDPR

Recital (11): Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the **rights of data subjects** and the **obligations of those who process and determine the processing of personal data**, as well as equivalent **powers for monitoring and ensuring compliance** with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.



The core data protection principles

Core data protection principles (Art. 5, GDPR)

- Lawfulness;
- Fairness;
- Transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality (security);
- Accountability;
- Data protection-by-design & by-default.

Lawfulness

Article 6

Lawfulness of processing

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

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

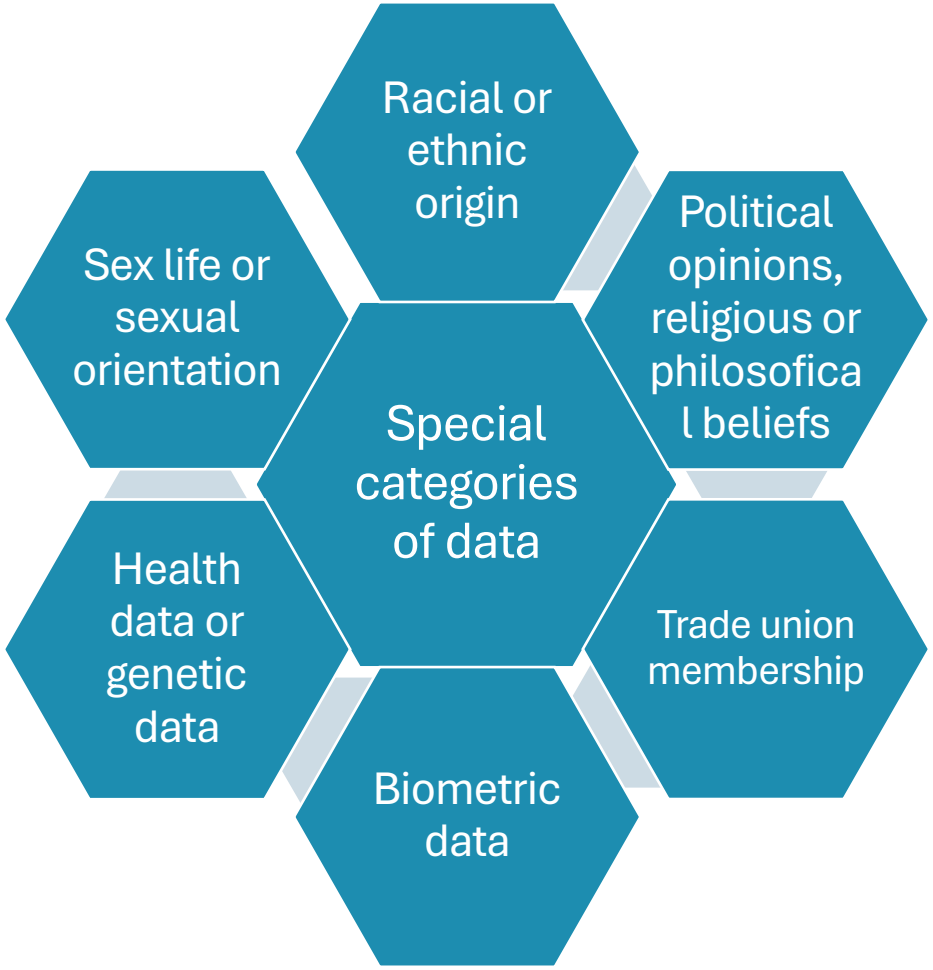
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

“Additional justification” for special categories of data

+ Data related to criminal convictions and offences (Art. 10)
+ Data related to children (Art. 8)
+ International personal data transfers (Chapter V)



Fairness

- Fairness ensures that individuals are not **unjustly** affected by the data processing;
- Discriminatory results;
- Reasonable expectations of data subjects.

- Important scenarios of application:
  - Automated decision-making;
  - Dark-patterns;
  - Processing children's data.

Transparency

- Individuals need to be informed about key aspects of data processing activities to exercise some control:
  - Who is processing the data?
  - What personal data are collected?
  - Why personal data are collected?
  - How are personal data being processed?
  - What are the rights of the data subject?

Purpose specification and limitation

- Purpose specification: data must be collected for specified, **explicit and legitimate** purposes.
  - To be specified in the moment of collection at the latest.
  - Data are not to be collected only later to be defined the purpose.

- Purpose limitation: Data must not be further processed in a manner that is incompatible with those initial purposes (compatibility test).

Data minimization

- Only data that is **adequate, relevant, and necessary** for the specified purpose should be processed.
- This principle aims to prevent excessive or irrelevant data collection, ensuring that organizations limit the amount of personal data they handle.

Accuracy

- Data must be accurate and, where necessary, kept up to date.
- Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Processing inaccurate data might be harmful for the data subjects. E.g.:
  - Credit score – Inaccurate data may lead to the denial of loans or unfavorable financial terms;
  - Medical records – Errors can result in incorrect treatments or dangerous medical decisions;
  - Criminal records – False information could negatively affect job prospects or other opportunities.

Storage limitation

- Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Directly linked with purpose specification and data minimization principles.

Integrity and confidentiality

- Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- The role of technical standards.

Accountability

- The controller shall be responsible for and be able to demonstrate compliance with the previous principles.
  - Records of the data processing activities within an organization.
- The role of the DPO.

Data Protection by design & by default

- Data protection by design: privacy and data protection issues should be considered at the earliest stages of products and services development.
- Data protection by default: only personal data which are necessary for each specific purpose of the processing are processed. This should be done automatically, without demanding individuals to take additional actions.

DPC fines TikTok €345 million for violations of children's data

The Inquiry

The DPC examined how TikTok processed children's data by looking at:

- Platform settings for child users, including the Family-Pairing setting;
- Age verification; and
- Transparency information for children.

The Time Period

The DPC launched an investigation into TikTok in Sept 2021 and examined how TikTok processed children's data between **31 July and 31 Dec 2020.**

The Findings

The profile settings for child user accounts were set to public by default, meaning anyone (on or off TikTok) could view the content posted by the child user.

The 'Family Pairing' setting allowed a non-child user (who could not be verified as the parent or guardian) to pair their account to a child user's account. This allowed the non-child user to enable Direct Messages for child users above the age of 16, which posed severe possible risks to child users.

The fact that profile settings for child users were set to public by default also posed several possible risks to children under the age of 13 who gained access to the platform.

TikTok failed to provide sufficient transparency information to child users.

TikTok implemented 'dark patterns' by nudging users towards choosing more privacy-intrusive options during the registration process, and when posting videos.

DPC fines TikTok €345 million for violations of children's data

The Inquiry

The DPC examined how TikTok processed children's data by looking at:

- Platform settings for child users, including the Family-Pairing setting;
- Age verification; and
- Transparency information for children.

The Time Period

The DPC launched an investigation into TikTok in Sept 2021 and examined how TikTok processed children's data between **31 July and 31 Dec 2020.**

The Findings

The profile settings for child user accounts were set to public by default, meaning anyone (on or off TikTok) could view the content posted by the child user.

- Articles infringed: 25(1), 25(2), 5(1)(c), and 24(1)

→ Data minimization

The 'Family Pairing' setting allowed a non-child user (who could not be verified as the parent or guardian) to pair their account to a child user's account. This allowed the non-child user to enable Direct Messages for child users above the age of 16, which posed severe possible risks to child users.

- Articles infringed: 5(1)(f) and 25(1)

→ Integrity and confidentiality

The fact that profile settings for child users were set to public by default also posed several possible risks to children under the age of 13 who gained access to the platform.

- Articles infringed: 24(1)

TikTok failed to provide sufficient transparency information to child users.

- Articles infringed: 12(1) and 13(1)(e)

→ Transparency

TikTok implemented 'dark patterns' by nudging users towards choosing more privacy-intrusive options during the registration process, and when posting videos.

- Articles infringed: 5(1)(a)

→ Fairness

Thank you!

KU Leuven Centre for IT & IP Law (CiTiP) - imec
Sint-Michielsstraat 6, box 3443
BE-3000 Leuven, Belgium

http://www.law.kuleuven.be/citip

imec KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW