L1 - Key notions in EU data protection law. Scope of application and data protection principles

Course: Data Science Regulation and Law

Cluster: Privacy and Data Protection

15 May 2024

TILBURG UNIVERSITY

Understanding Society

Privacy and Data Protection

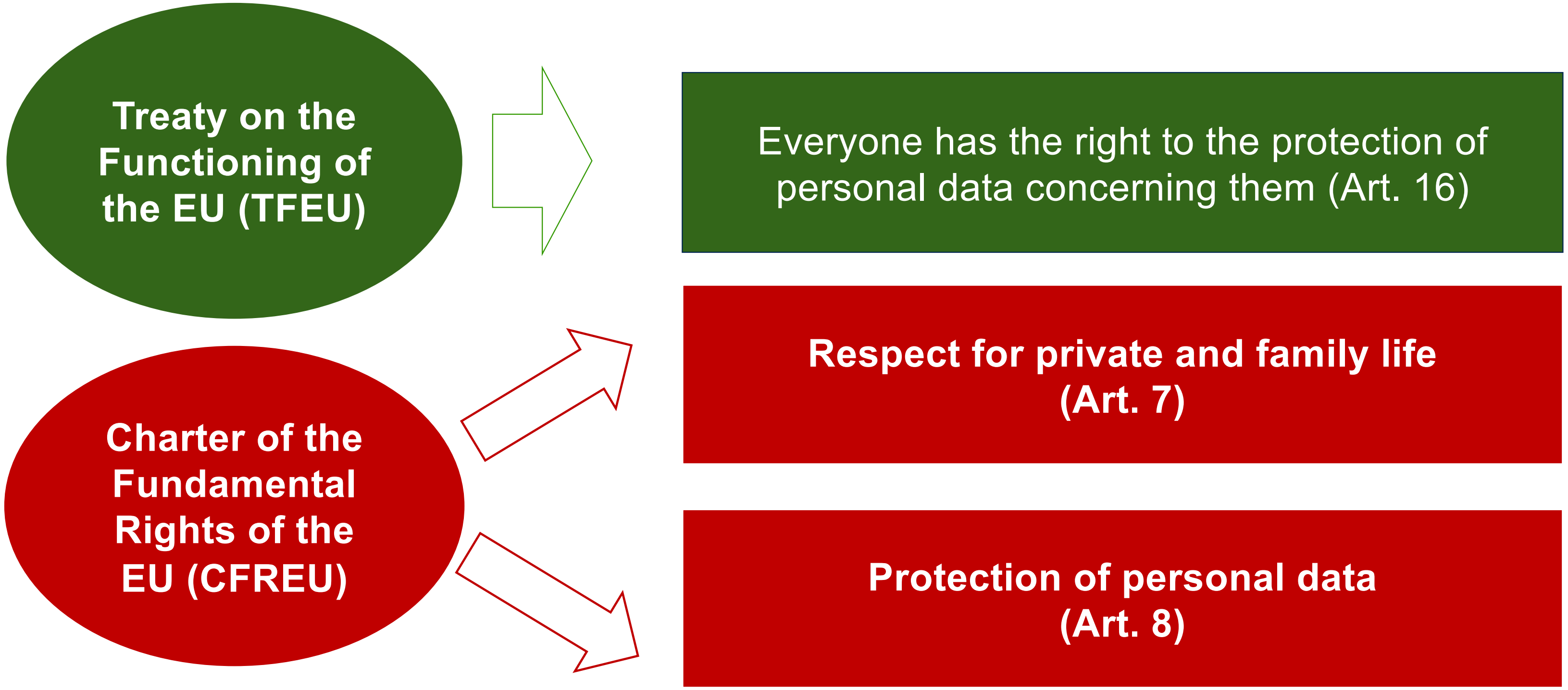
Right to privacy

Right to be let alone is conceived as the freedom from any unauthorized intrusion or interference by public and private bodies into private life

Right to data protection

It is based on the concept of personal data, requires that the (authorized) use of the same by private and public bodies is made in accordance with specific legal standards

Privacy and Data Protection



Treaty on the Functioning of the EU (TFEU)

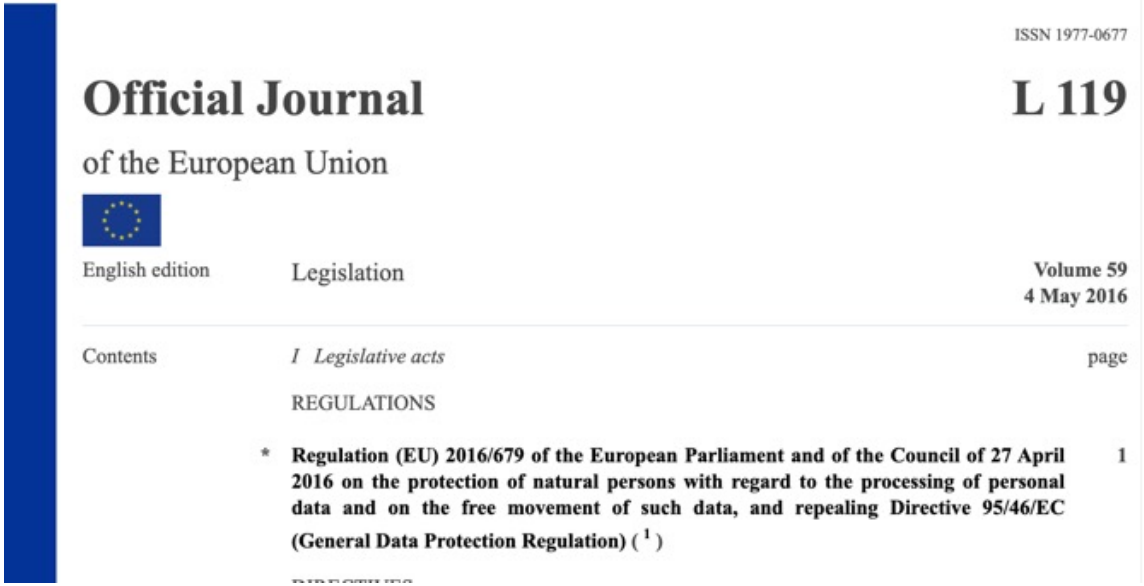
Everyone has the right to the protection of personal data concerning them (Art. 16)

Charter of the Fundamental Rights of the EU (CFREU)

Respect for private and family life (Art. 7)

Protection of personal data (Art. 8)

The General Data Protection Regulation



ISSN 1977-0677

Official Journal

of the European Union

L 119

English edition

Legislation

Volume 59
4 May 2016

Contents

I Legislative acts

page

REGULATIONS

* **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ([1])** 1

DIRECTIVES

Scope of application

GDPR: scope of application

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.
2. […]

GDPR: scope of application

<u>Processing</u> of personal data

"**<u>any operation</u>** or set of operations which is **<u>performed on personal data</u>** 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*" (Art. 4 GDPR)

GDPR: scope of application

Processing of **personal data**

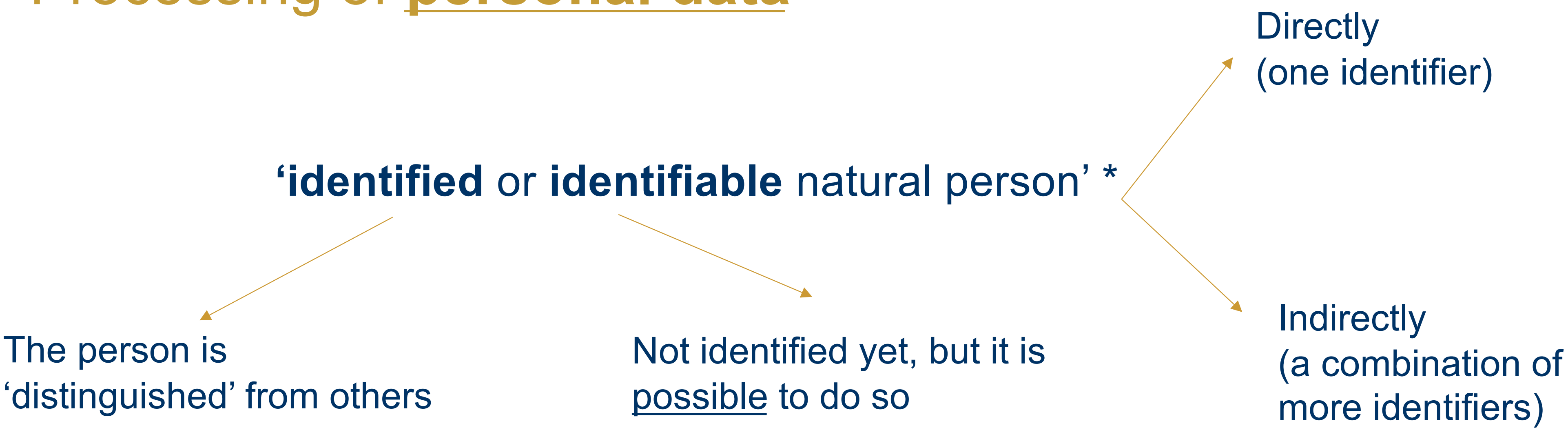
‘**personal data**’ means **any information** ***relating to*** an **identified** or **identifiable** natural person (‘**data subject**’) (Art. 4 GDPR)

Data subjects=living individuals. GDPR is not applicable to deceased persons

Examples: name; identification number (e.g. social security number); online identifier (e.g. IP address); images; sounds; fingerprints; DNA

GDPR: scope of application

Processing of **personal data**



‘**identified** or **identifiable** natural person’ *

Directly
(one identifier)

Indirectly
(a combination of
more identifiers)

The person is
‘distinguished’ from others

Not identified yet, but it is
possible to do so

* Taking into consideration:
(1) the available technology at the time of the processing and technology developments, and
(2) the means reasonably likely to be used (for identifiable)

GDPR: scope of application

Processing of **personal data**

Identifiers include, e.g.: name, an identification number; location data; age; any factor specific to the physical, physiological, genetic, mental, economic, cultural, or social identity

GDPR: scope of application

Processing of **personal data**

- Any information has the potential to be personal data, but the assessment is **situational (= in light of all circumstances of a situation)**
- **Anonymous data** is not personal data, so the GDPR does not apply
- But **pseudonymous data** is personal data

Pseudonymisation is the processing of personal data in such a way that this data can no longer be attributed to a specific individual, without the use of additional information.

What differs pseudonymisation from anonymisation is that the latter consists of removing personal identifiers, aggregating data, or processing this data in a way that it can no longer be related to an identified or identifiable individual

GDPR: scope of application

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.
2. […]

GDPR: scope of application

Material scope: exceptions

The GDPR does not apply to the processing of personal data:

- in the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities which fall within the scope of the Common Foreign and Security Policy;
- **by a natural person in the course of a purely personal or household activity;**
- 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 [Directive 680/2016]

GDPR: scope of application

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. […]

GDPR: scope of application

Territorial scope

- The GDPR applies to organizations with EU establishments if the processing of personal data occurs in the context of the activities of such an establishment (see *Google Spain*)
  - Broad and flexible concept of "establishment": an organization is established **when it exercises a real and effective activity through stable arrangements in the EU** (see *Weltimmo*)

- **Non-EU established organizations are subject to the GDPR where they process personal data concerning EU data subjects in connection with the offering of goods or services or monitoring their behavior within the EU**

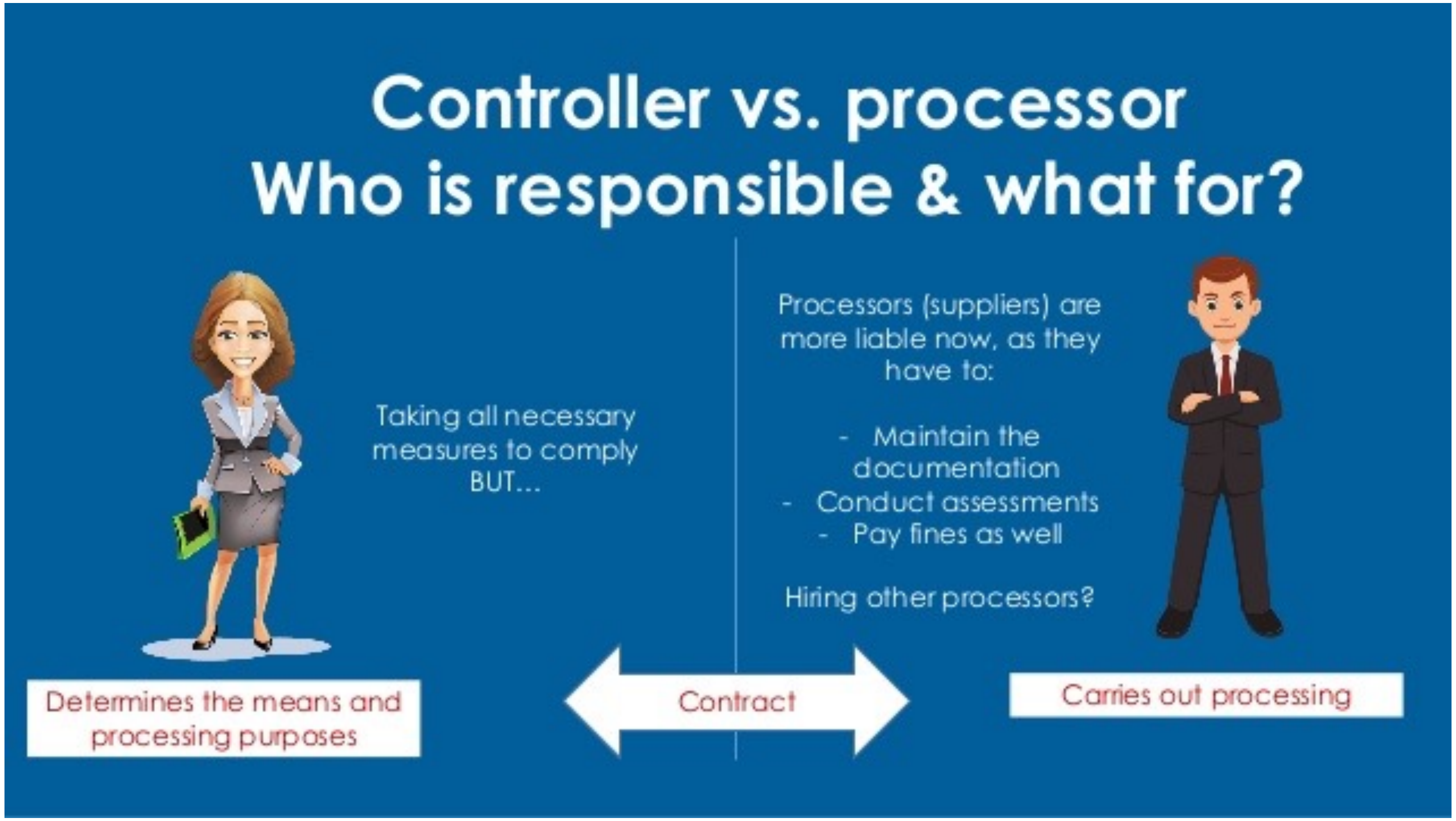
Actors in EU data protection law

Controller and Processor

‘**controller**’ means the natural or legal person, public authority, agency or other body which, **alone or jointly** with others, **determines the purposes and means** of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

‘**processor**’ means a natural or legal person, public authority, agency or other body which processes personal data **on behalf of the controller**;

Controller and Processor



Controller vs. processor
Who is responsible & what for?

Taking all necessary measures to comply BUT…

Processors (suppliers) are more liable now, as they have to:

- Maintain the documentation
- Conduct assessments
- Pay fines as well

Hiring other processors?

Determines the means and processing purposes

Contract

Carries out processing

Controller and Processor: examples

An ISP providing hosting services is in principle a **processor** for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If however, the ISP further processes for its own purposes the data contained on the websites then it is the data **controller** with regard to that specific processing.

The provider of telecommunications services should, in principle, be considered **controller** only for traffic and billing data, and not for any data being transmitted.

The owner of a building concludes a contract with a security company, so that the latter installs some cameras in various parts of the building on behalf of the controller. The purposes of the video-surveillance and the way the images are collected and stored are determined exclusively by the owner of the building, which therefore has to be considered as the sole **controller** for this processing operation.

A data controller outsources some of its operations to a call centre and instructs the call centre to present itself using the identity of the data controller when calling the data controller's clients. In this case the expectations of the clients and the way the controller presents himself to them through the outsourcing company lead to the conclusion that the outsourcing company acts as a data **processor** for (on behalf of) the controller.

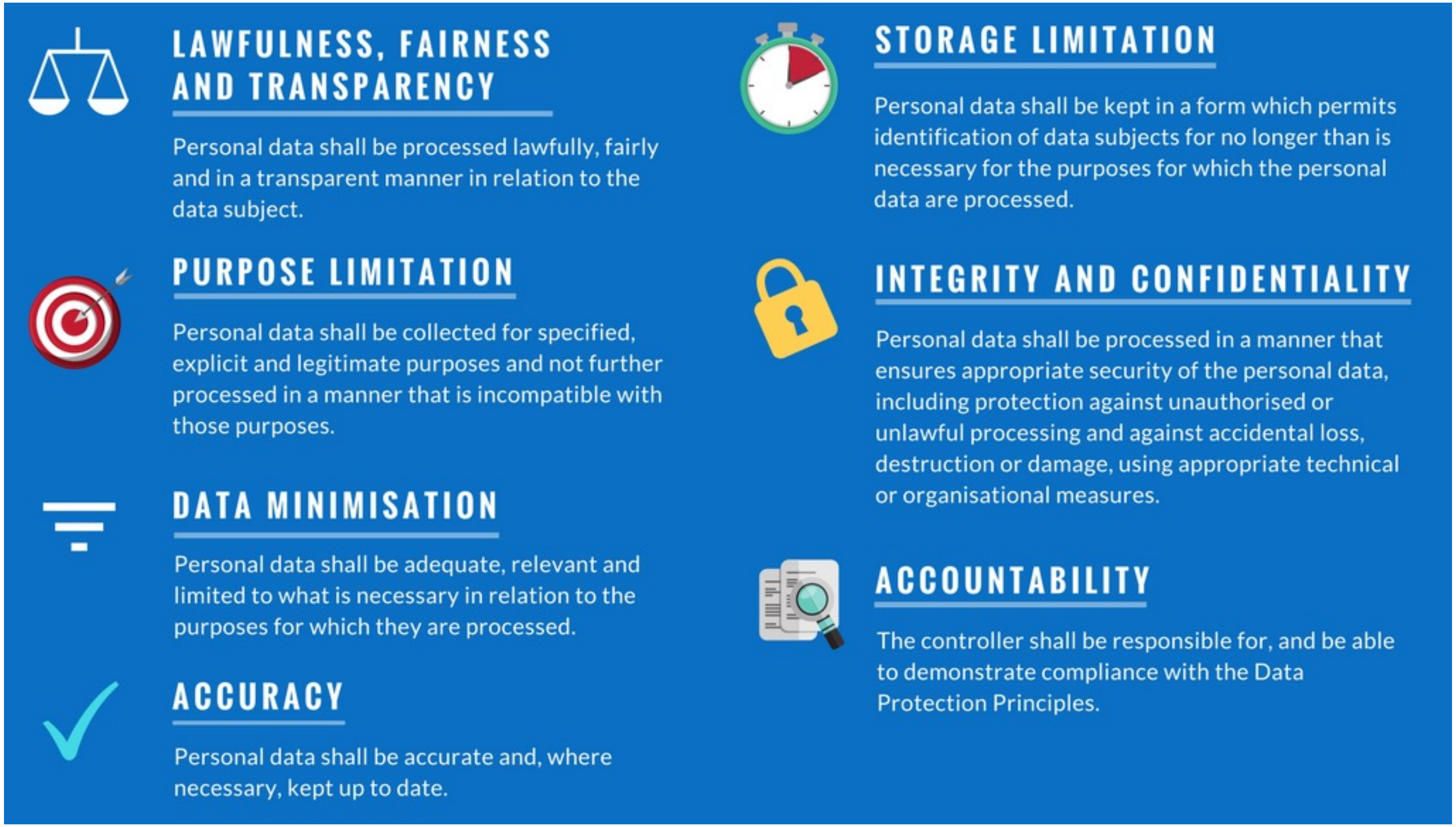
Other actors in data protection law

Data Protection Officers (DPO)

AUTORITEIT
PERSOONSGEGEVENS

Data protection principles

Data protection principles



LAWFULNESS, FAIRNESS AND TRANSPARENCY

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

PURPOSE LIMITATION

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

DATA MINIMISATION

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

ACCURACY

Personal data shall be accurate and, where necessary, kept up to date.

STORAGE LIMITATION

Personal data shall 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.

INTEGRITY AND CONFIDENTIALITY

Personal data shall 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.

ACCOUNTABILITY

The controller shall be responsible for, and be able to demonstrate compliance with the Data Protection Principles.

1. Lawfulness, transparency and fairness

- **Lawfulness** – a legal ground is required to justify the processing of personal data
- **Transparency** – data subjects need to be informed about how their personal data are processed in clear and simple language - so they need to understand how their data are being used by the data controller
- **Fairness** – personal data must be processed in a transparent and even ethical manner

2. Purpose limitation

- Data controllers must determine, **in advance** of any processing, why they want to process certain personal data.
- The purpose chosen needs to be **specific** and **clear** so that data subjects know what to expect.
  - Processing personal data for undefined/vague purposes is unlawful (would be equal to processing data on the basis that they may be useful in the future)
- Also, personal data shall not be further processed in a manner that is incompatible with those purposes

Purposes that are *always* compatible:

- Archiving purposes in the public interest
- Scientific or historical research purposes
- Statistical purposes

2. Purpose limitation: assessing compatibility

A vegetable box online retailer delivers an organic box each week to customers' homes. After the initial **collection** of the customers' address and banking information, the company wants to implement an off-the-shelf price-customization software that uses collected data *and* data on device type (i.e., whether an Apple or Windows computer is used) to automatically give greater discounts to Windows users.

Is this a compatible purpose?

No. The further use of collected data and the collection of additional information for a purpose unrelated with the initial one (price discrimination) is problematic.

Article 29 Working Party, Opinion 03/2013 on purpose limitation

3. Data minimisation

- Data controllers should use as few personal data as possible for a specific purpose.
- This means that personal data shall be **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed.
- Exceeding data or data that has become irrelevant should be deleted as soon as possible

4. Accuracy

- Data controllers must make sure that the personal data they process are **accurate** and **up to date**.
- Data subject to processing activities must reflect reality.
- There are situations where this is more necessary than in others.
  - For example, banking institutions process individuals' credit history data. If these data are not kept accurate and up to date, data subjects may suffer negative effects, e.g., inability to obtain credit.
- Every reasonable step must be taken to ensure that data that is inaccurate, having regard to the purposes of the processing, is **erased or rectified without delay.**

5. Storage limitation

- Data controllers must only keep personal data for the duration for which the processing is **necessary** for the **purpose** for which data has been collected. This means not keeping data when they the processing is no longer necessary for the purpose.
- Data controllers need to establish **time limits** for keeping the data and **erasing** them permanently when they are no longer necessary (data retention)

6. Integrity and confidentiality

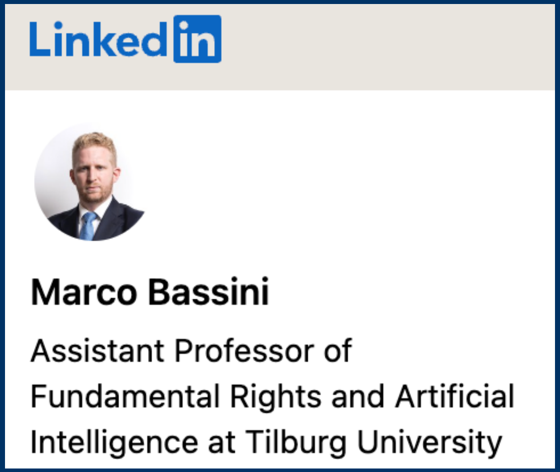
- Data controllers need to make sure that the processing of personal data ensures **adequate security**, by putting in place technical and organizational measures
- **Technical measures** – e.g., encryption, pseudonymization
- **Organizational measures** – e.g., placing personal data copies in a locked room inside the office building, only giving permissions to access the data to certain employees that need it to carry out their tasks
- The goal of such measures is to prevent unlawful processing of data, modification, loss, destruction, damage
  - if this occurs, then the **data breach** must be **notified** to the Supervisory Authority in 72 hours. Also, if the breach is likely to result in a high risk to the rights and freedoms of natural persons, data subjects must also be **communicated** to the data subjects.

7. Accountability

- Data controllers are responsible for compliance with data protection law rules and must be able to **demonstrate compliance**.
- Compliance can be demonstrated by maintaining a **record of all processing activities** the company carries out, which includes information such as:
  - purposes for processing
  - categories of personal data
  - transfers of personal data
  - time limits for erasure
  - technical and organizational measures to secure the data
- Other ways to demonstrate compliance: if relying on consent, must demonstrate valid consent has been obtained; if relying on legitimate interest, must demonstrate balancing exercise was carried out, etc.

7. Accountability

- **Risk-based approach**: required level of data security must be identified **on a case-by-case basis** through an objective **risk assessment.**
- The GDPR encourages controllers to engage in **risk analysis** and to adopt **risk-measured responses**. It imposes additional obligations for data processing activities that pose a high risk to individuals, while requiring controllers to **account** for risk in complying with many provisions of the GDPR.



LinkedIn

Marco Bassini

Assistant Professor of Fundamental Rights and Artificial Intelligence at Tilburg University

Thank you!
m.bassini@tilburguniversity.edu