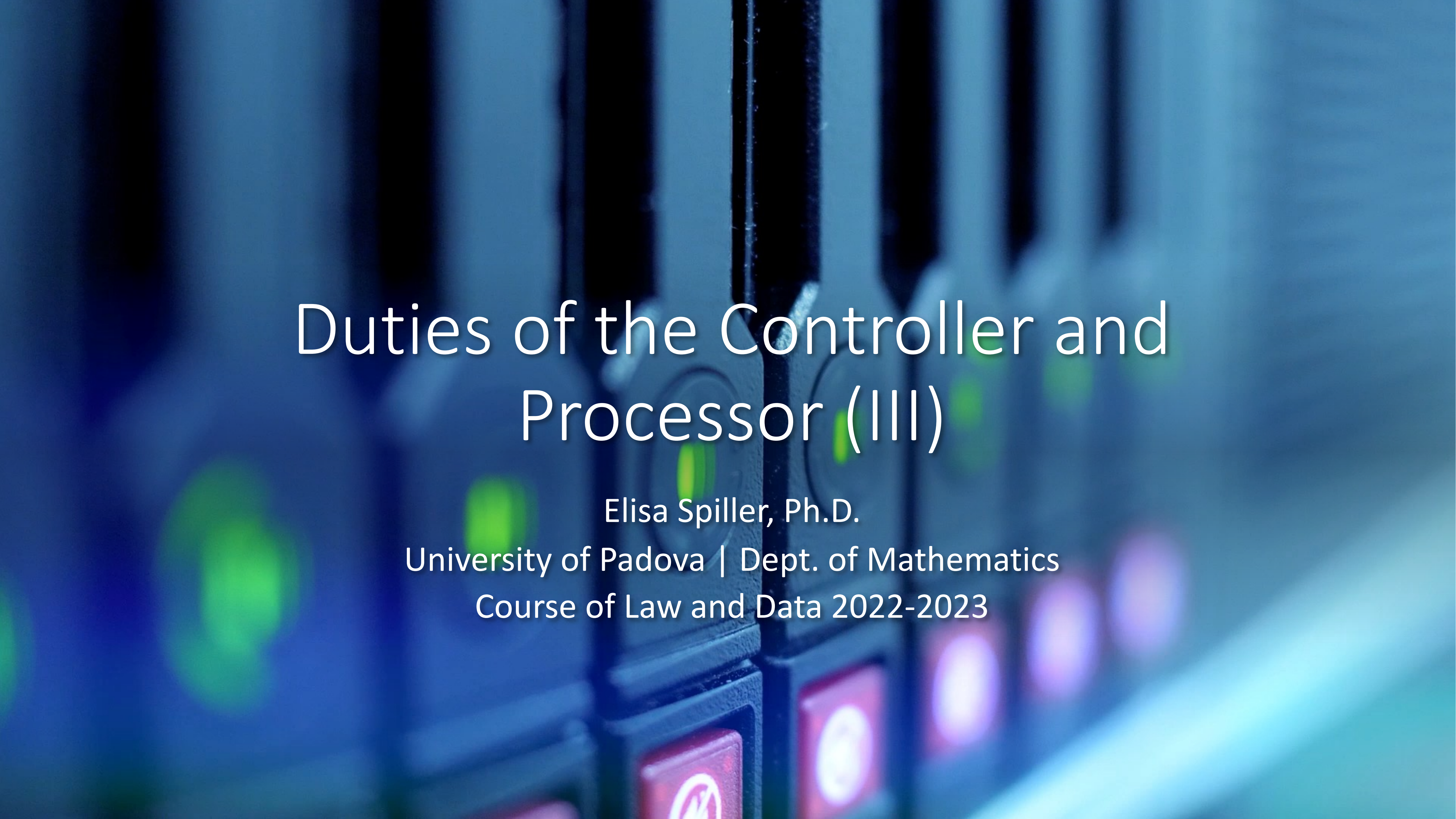


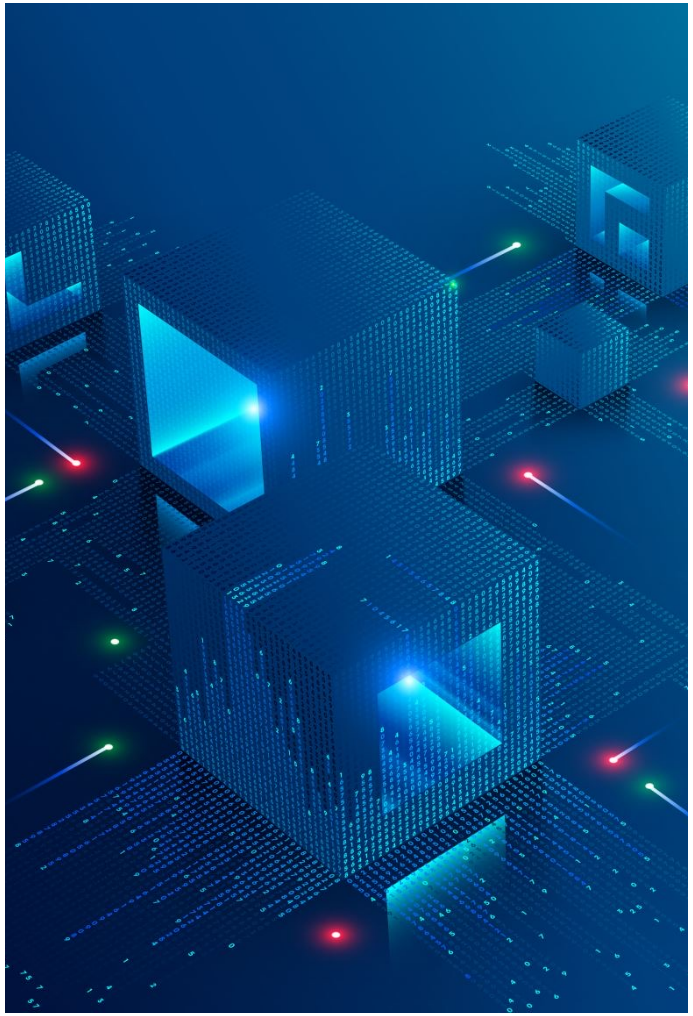
Duties of the Controller and Processor (III)

Elisa Spiller, Ph.D.
University of Padova | Dept. of Mathematics

Course of Law and Data 2022-2023

learning objectives

- introduction: protection by design
- data protection by design
- AI and protection by design

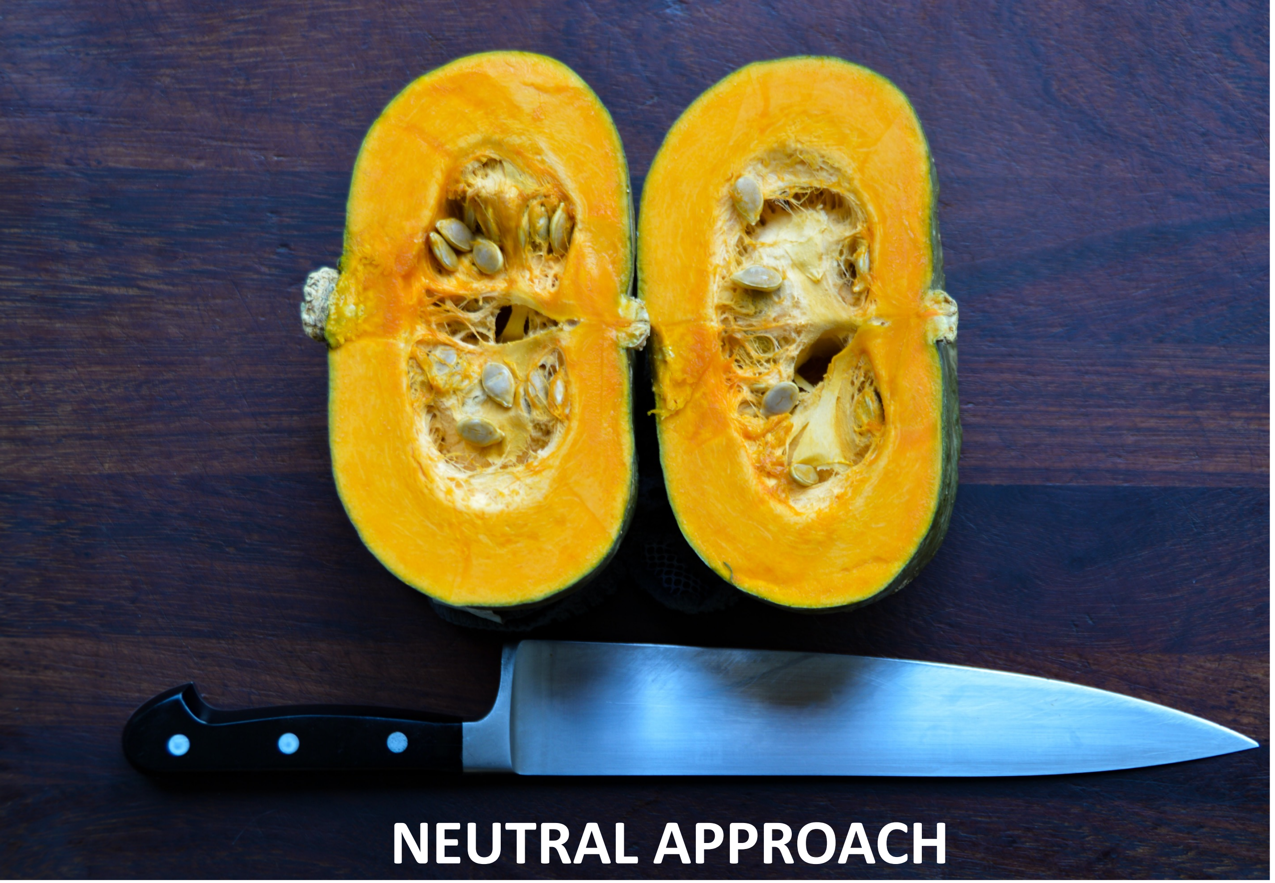


1. Protection by design (intro)

Design

Normative Design

Normative Design



NEUTRAL APPROACH

REGULATORY APPROACH

Regulating Design

People Environment Design

2. privacy and data protection by design

Privacy Enhancing Technologies

- a method of protecting data building legal principles into information system architecture
- minimize possession of personal data without losing the functionality of an information system
- hard and soft privacy technologies
- increasing control over personal data (informational self-determination)
- minimize personal data collected and used by service providers and merchants
- use pseudonyms or anonymous data credentials to provide anonymity
- strive to achieve informed consent about giving personal data to online service providers and merchants

Design as Software architecture

What is software architecture? (Shaw and Garlan 1996)

- “Software architecture encompasses the **set of significant decisions** about the organization of a software system including the **selection of the structural elements** and their **interfaces** by which the system is **composed**;”
- “behavior as specified in **collaboration among those elements**; composition of these structural and behavioral elements into **larger subsystems**;”
- “and an architectural **style that guides** this organization.”

Architecture should:

- **Expose the structure** of the system but **hide the implementation** details.
- Realize all of the **use cases** and scenarios.
- Try to **address the requirements** of various stakeholders.
- Handle both **functional** and **quality** requirements.

Legal or Ethical Requirements?

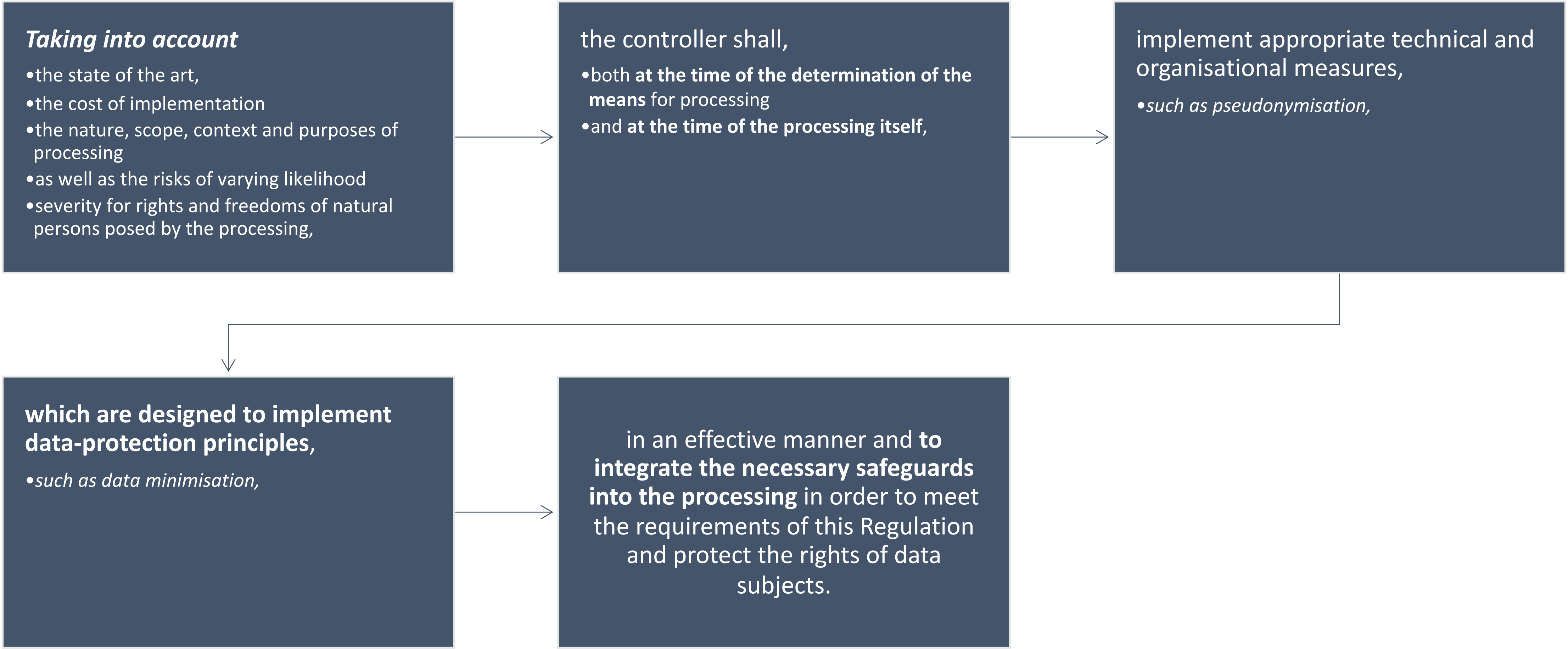
«‘value sensitive by design’ or ‘privacy by design’ [are] often proposed as *ethical requirements,* which is problematic for two main reasons.

1. First, as *ethical norms cannot level the playing field*, companies that apply such ethical design may be pushed out of the market.
2. Second, *ethical ‘by design’ approach make protection dependent on the ethical inclination* of those who develop and market the choice architecture

Data protection by design & by default

- *Article 25*
- **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. The 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. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In 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.
- 3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

Data Protection By Design & By Default



Taking into account

- the state of the art,
- the cost of implementation
- the nature, scope, context and purposes of processing
- as well as the risks of varying likelihood
- 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,

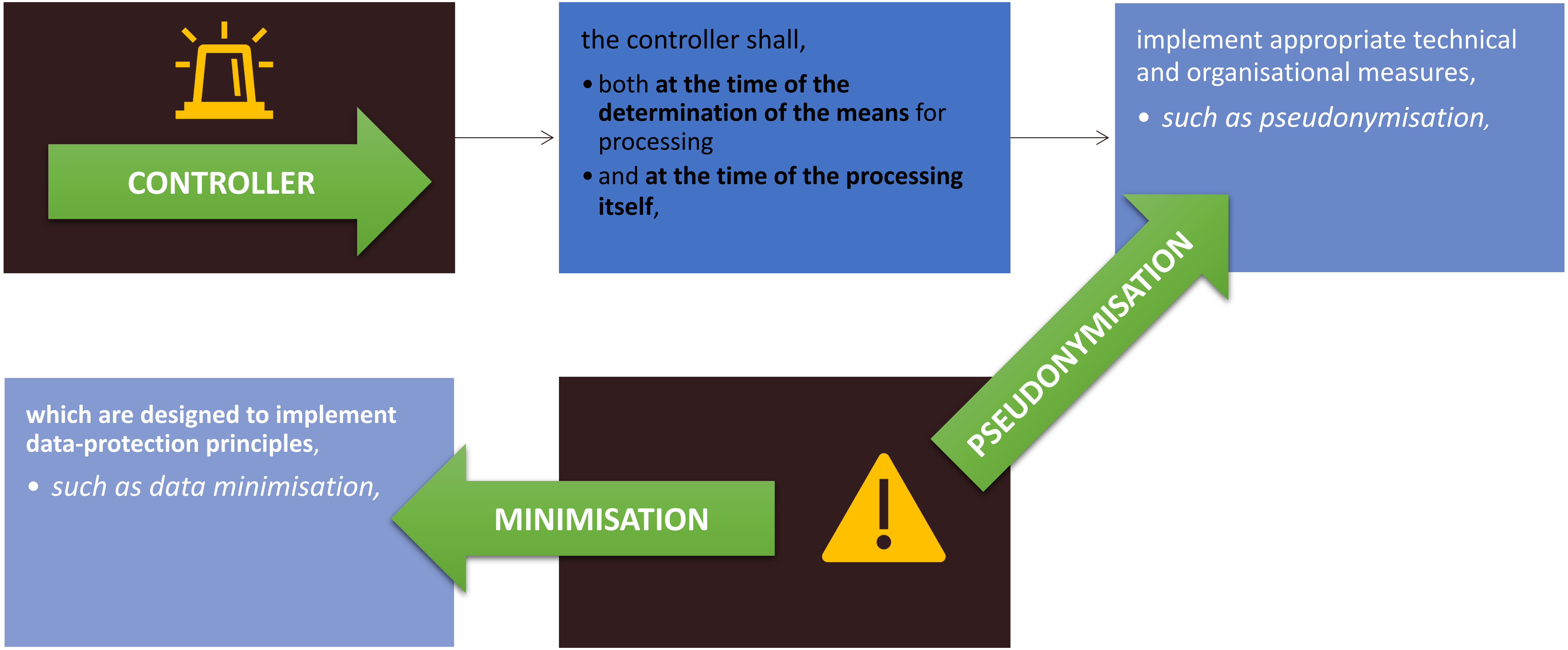
- *such as pseudonymisation,*

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.

Data Protection By Design & By Default



CONTROLLER

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,*

PSEUDONYMISATION

MINIMISATION

which are designed to implement data-protection principles,

- *such as data minimisation,*

3. AI & design

What is different?

- Data
- Process
- Automation
- Autonomy