KU LEUVEN CiTiP

CENTRE FOR IT & IP LAW

imec

KU Leuven Centre for IT & IP Law (CiTiP) – imec

www.law.kuleuven.be/citip

Purpose AI Act

- Harmonised rules for placing on the market, putting into service and using AI systems
- Prohibition of certain AI practices
- Specific requirements for high-risk AI systems and obligations for operators of such systems
- Harmonised transparency rules
  - AI systems intended to interact with natural persons
  - Emotion recognition systems and biometric categorisation systems
  - AI systems used to generate or manipulate image, audio or video content
- Rules on market monitoring and surveillance

Status AI Act

European Commission

Proposal AI Act

April 2022

European Council

General Approach

December 2022

European Parliament

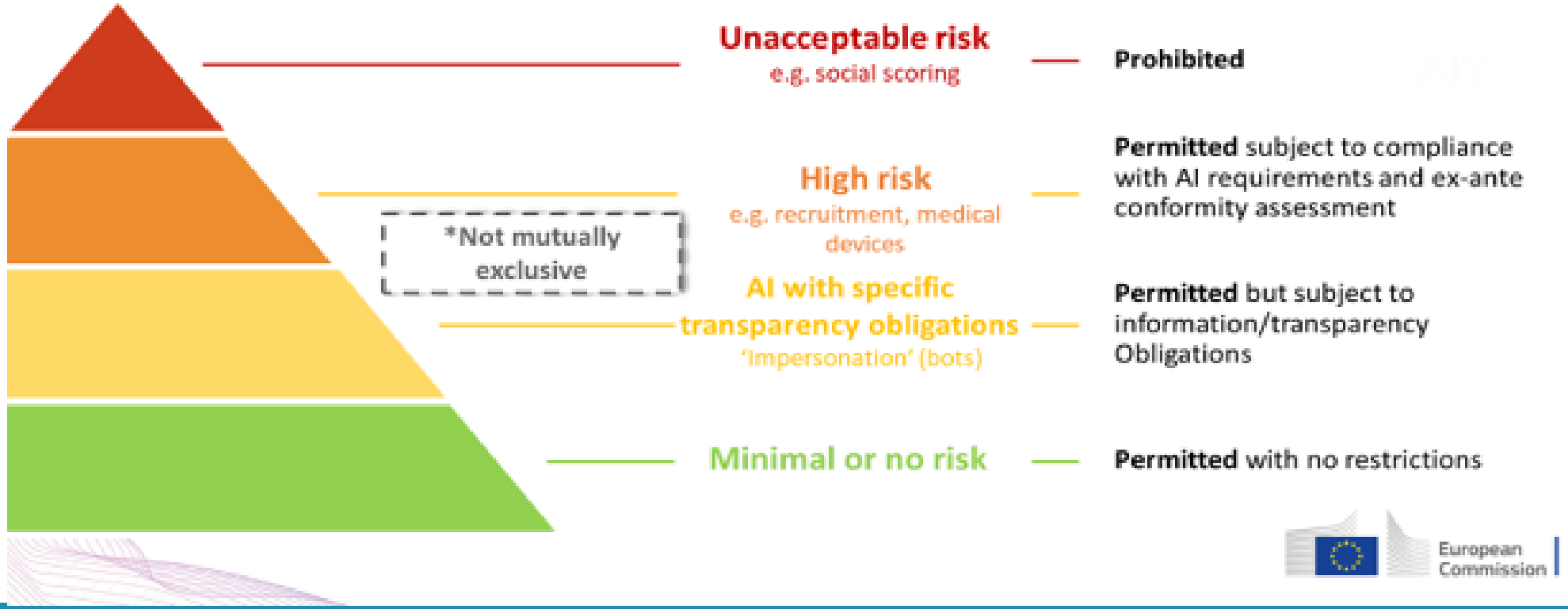
Position

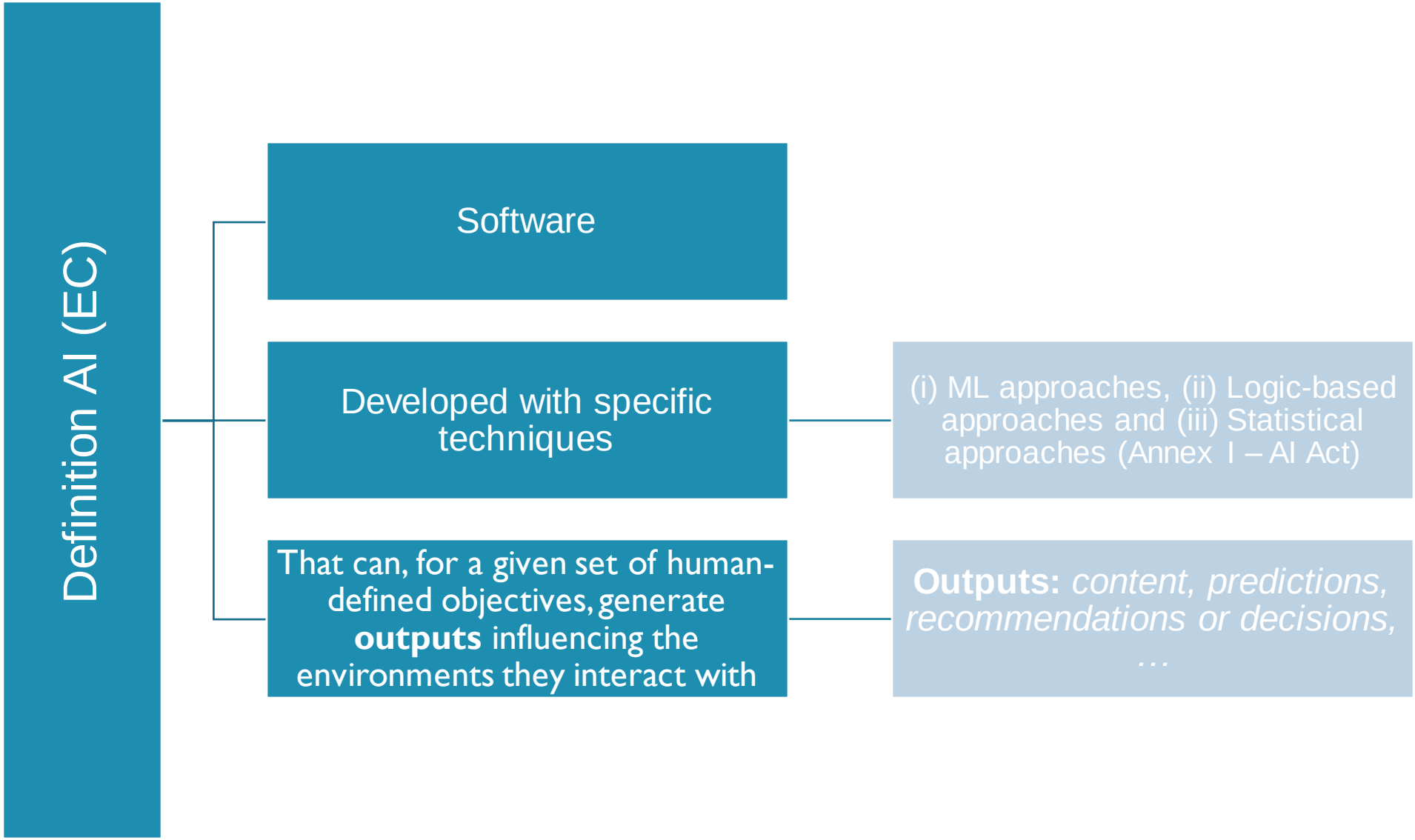
June 2023

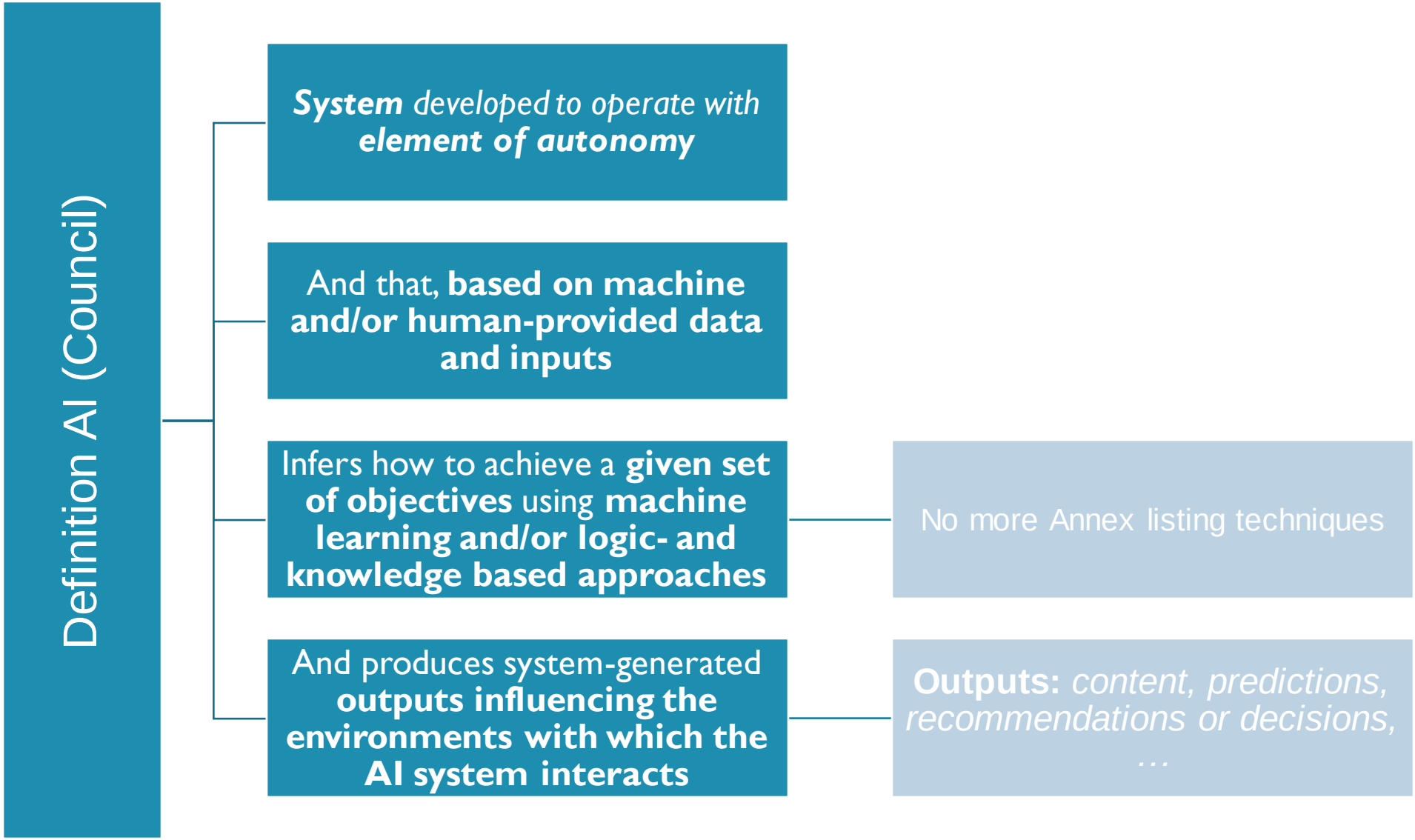
- Trilogue → final text before end of 2023? Before European elections?
- Application: 24 months (EC/CP)/36 months (Council) after entry into force

AI Act proposal

A risk-based approach to regulation

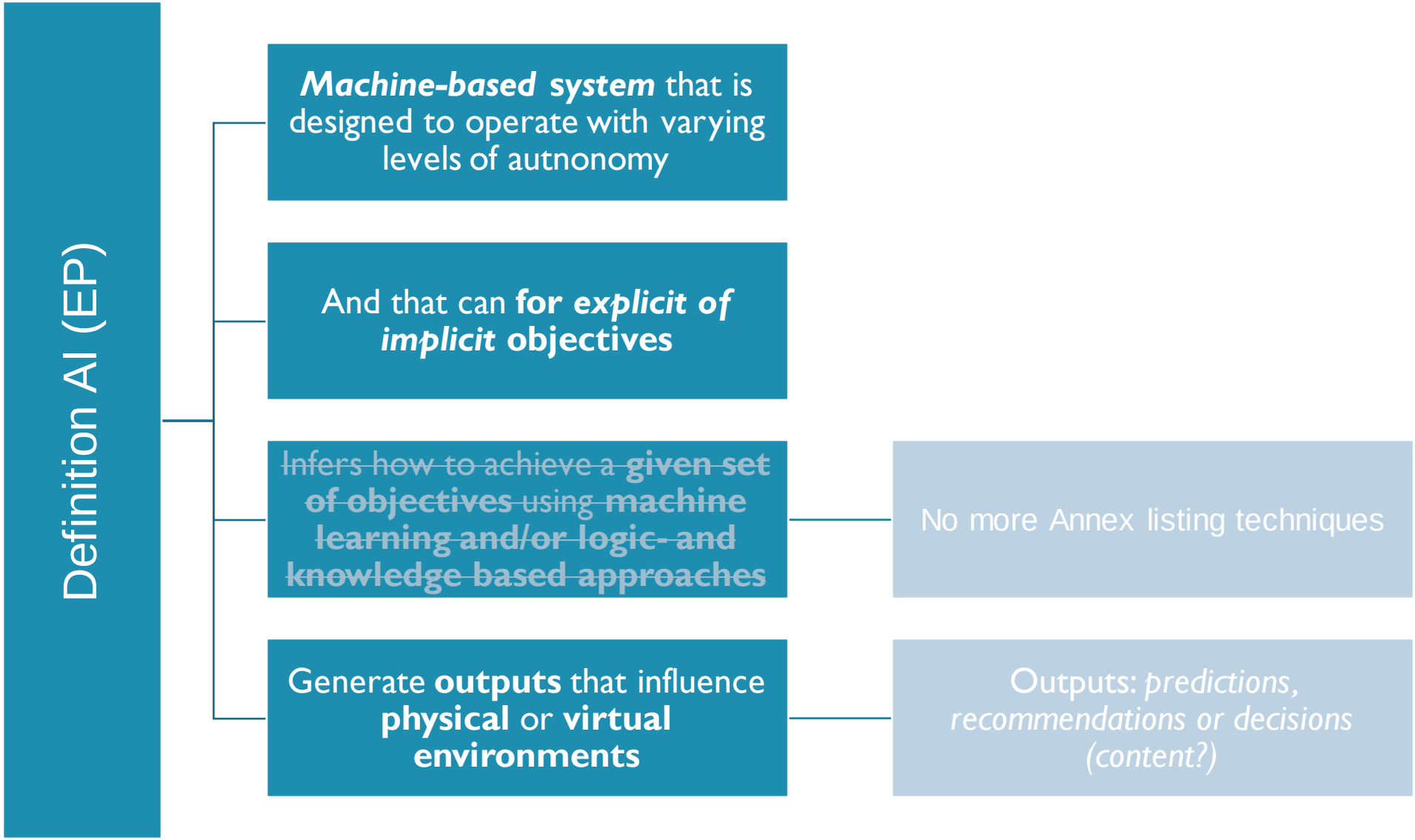



Definition AI (EC)
Software
Developed with specific techniques
(i) ML approaches, (ii) Logic-based approaches and (iii) Statistical approaches (Annex I – AI Act)
That can, for a given set of human-defined objectives, generate **outputs** influencing the environments they interact with
Outputs: *content, predictions, recommendations or decisions, …*



imec

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW


Definition AI (EP)
Machine-based system that is designed to operate with varying levels of autnonomy
And that can **for *explicit of implicit* objectives**
~~Infers how to achieve a **given set of objectives** using **machine learning and/or logic- and knowledge based approaches**~~
No more Annex listing techniques
Generate **outputs** that influence **physical** or **virtual environments**
Outputs: *predictions, recommendations or decisions (content?)*

AI-research? (Council)

Exclusion of:

- AI systems (and their output) specifically developed and put into service for the sole purpose of scientific research and development
- Any research and development activity regarding AI systems

European Declaration of Digital Rights and Principles for the Digital Decade (Dec 2022)

- Chapter III: Commission, Council and EP "*commit to taking measures to ensure that research in artificial intelligence respects the highest ethical standards and relevant EU law*"

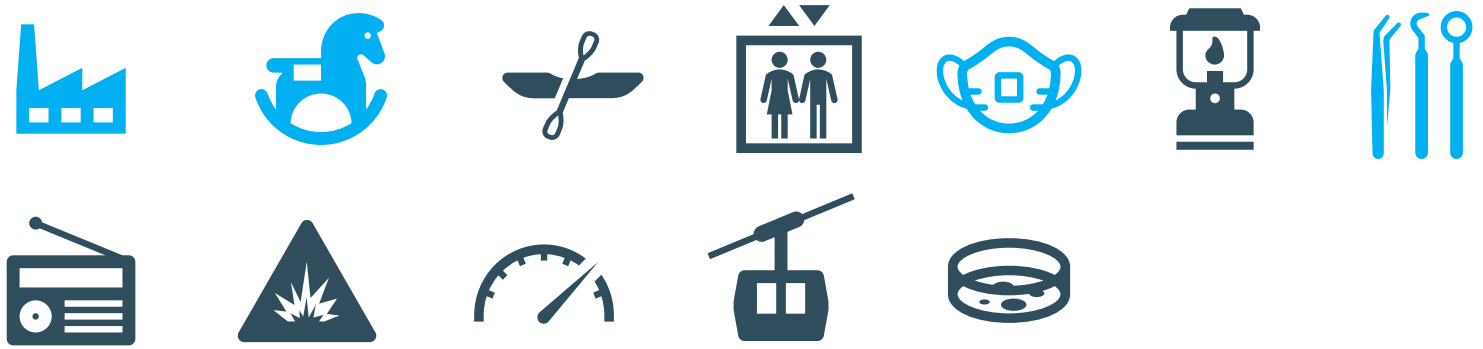
High Risk AI-systems

Type 1 High Risk

AI shall be considered high risk if:

- AIS intended to be used as a **safety component of a product**, or is **itself a product**, covered by the Union harmonisation legislation listed in Annex II
- **And** the product is required to undergo a third-party conformity assessment

Which products?



Type 2 High Risk (Annex III)

- **Biometric identification and categorisation of natural persons**
  - ‘Real time’ and ‘post’ remote biometric identification of natural persons
- **Management and exploitation of critical infrastructure:**
  - Safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity
- **Onderwijs en beroepsopleiding:**
  - Assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions
- **Access to and enjoyment of essential private services and public services and benefits**
  - Evaluate eligibility of natural persons for public assistance benefits and services
  - Evaluate the creditworthiness of natural persons or establish their credit score
- **Etc.**

High Risk AI-system (Council/EP)

- **Council**: nuance of HR type 2
  - *"unless the output of the system is purely accessory in respect of the relevant action or decision to be taken and is not therefore likely to lead to a significant risk to the health, safety or fundamental rights"*
- **EP**: addition to HR type 2
  - *"if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons"* **+** *melding aan toezichthouder*
  - Notification to the national supervisory authority (or AI Office) if not considered high risk

Requirements & obligations

Risk management system

- Continuous iterative process
- Entire lifecycle AIS
- Risk management measures
- Testing to identify the most appropriate measures

Data and data governance

- Appropriate data governance and management measures
- Quality requirements (*relevant, representative, free of errors and complete*)

Technical documentation

- Purpose: demonstrate compliance
- Details in Annex IV (development process, description of system architecture, validation and testing procedures used, …)

Record-keeping

- Purpose: ensuring a level of traceability of functioning AIS
- Automatic registration of events: "logs"
- Minimal requirements for biometrische identification

Transparency and provision of information to users

- Purpose: *enable users to interpret the system's output and use it appropriately*
- Instructions for use
  - Minimal information, e.g., intended purpose, level of accuracy, …

Human oversight

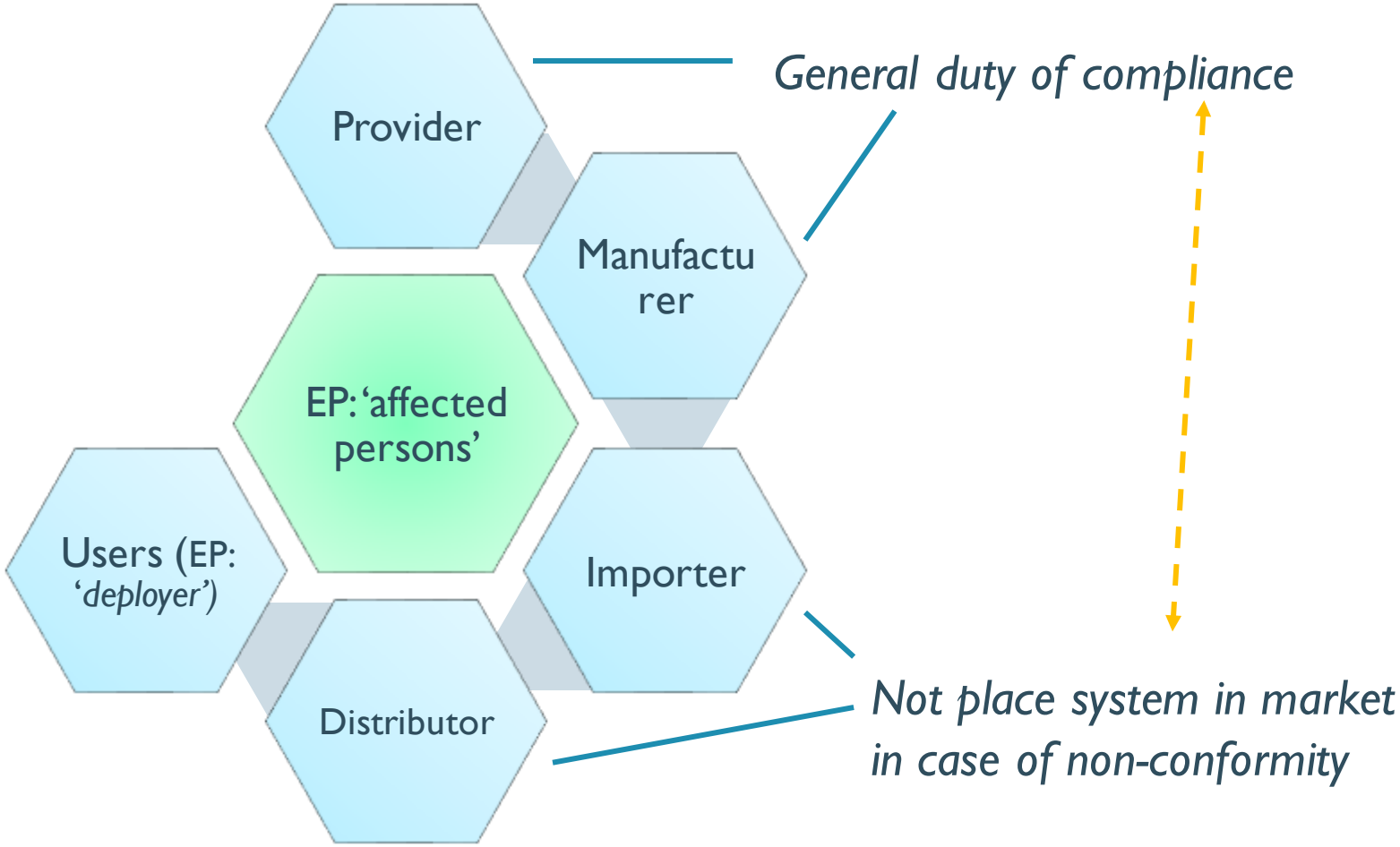
- Purpose: *allow effective oversight by natural persons*
- Built-in or to be implemented by user
- Minimal requirements, e.g., monitoring of operation, correct interpretation of output, override or reverse output, …

Accuracy, robustness and cybersecurity

- Accuracy declared in instructions of use
- Robustness: e.g., address "*feedback loops*"
- Cybersecurity: e.g., address vulnerabilities ("*data poisoning*", "*adversarial examples*", …)

Roles and responsibilities

Different actors (EC/Council)



Provider	Manufacturer	Importer	Distributor	User (deployer?)
General duty of compliance	General duty of compliance *(products Annex II – Section A + under name of Manufacturer)*	Technical documentation	CE-marking of conformity (+ use instructions)	Information duty à P & D authorities *(risks/incidents)*
Quality management *(prop. to size of organisation)*		Conformity assessment	Information duty à P, I & authorities *(risks)*	Record-keeping (if control)
(Technical) documentation		CE-marking of conformity (+ use instructions)	Cooperation with competent authorities	Cooperation with competent authorities
Record-keeping (if control)		Information duty à A & authorities *(risks)*	Corrective actions *(or by P/I)*	
Conformity assessment		Cooperation with competent authorities		
CE-marking of conformity		***Specific obligations***		
Corrective actions *(info → D&I)*		Indicate name and address *(Council: also providers)*	Appropriate storage and transport conditions	Human oversight, monitoring, use in accordance with instructions of use
Duty of information (inform comp. auth. of risks)		Appropriate storage and transport conditions		Relevant inputdata (if under their control)
Registration in HR DB				DPIA (if necessary)
Cooperation with competent authorities		*Keep AIS off the market in case of non-conformity*		Council: Registration in HR DB *(if public authorities)*

AI with specific transparency requirements
&
GPAI/FM

Art. 52

- **Interactive AI-systems**
  - *Inform natural persons of AI interaction(unless obvious)*
- **Biometric categorisation & emotion recognition**
  - *Inform natural persons exposed of operation*
- **Deep fakes**
  - *Inform of artificial nature of content*

Obligations for GPAI/FM

- **Council**
  - Specific obligations for providers ***General Purpose AI-systems*** (if high-risk use)

- **EP**
  - Specific obligations for providers of '***Foundational Models***'
  - Specific obligations regarding transparency of training data

Thank you

Bert.peeters@kuleuven.be

Slides based on a presentation courtesy of Thomas Gils and the Flemish Knowledge Center Data & Society

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

imec KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW