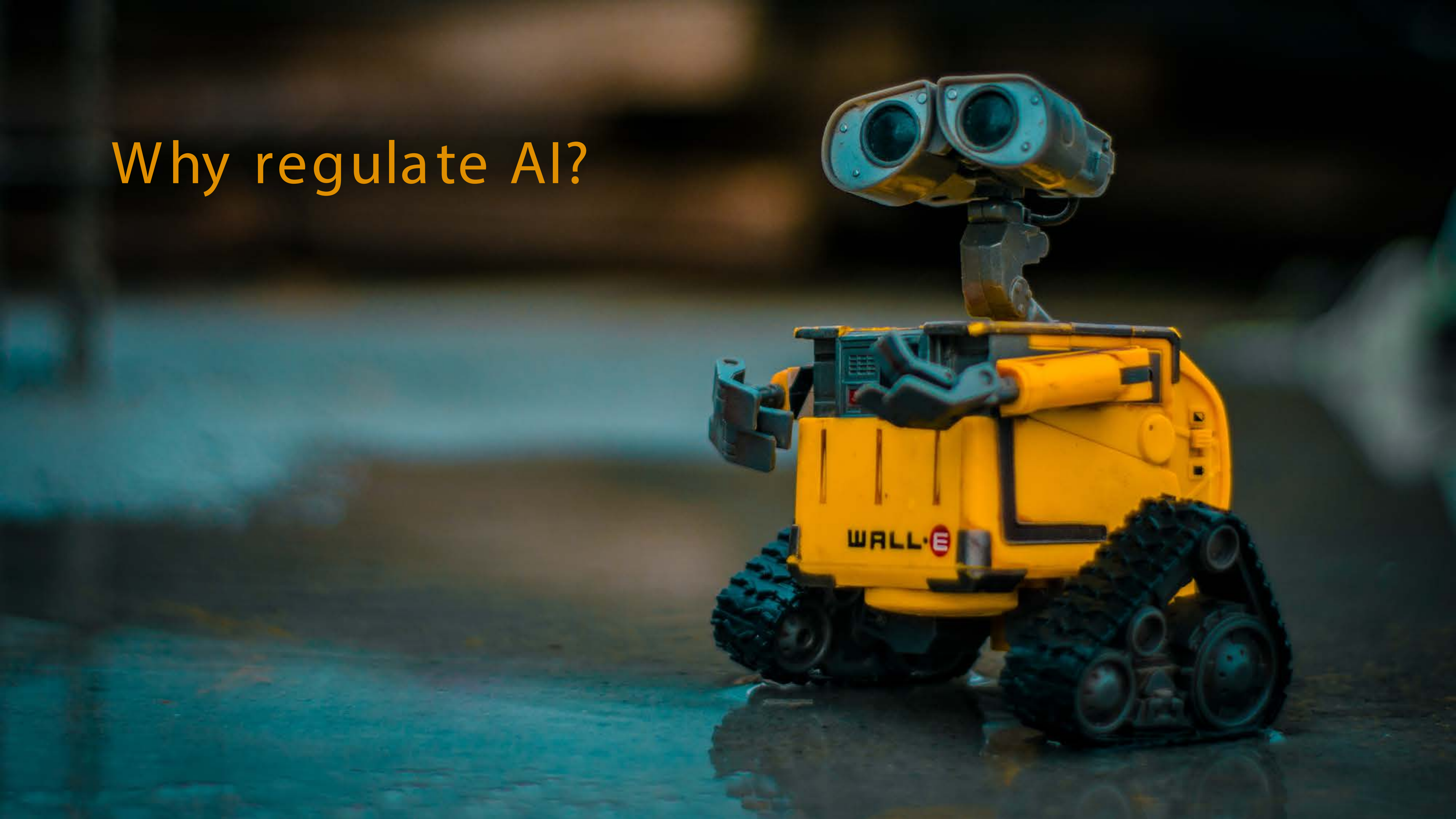
CULLEN INTERNATIONAL

# AI and the Data Economy

Philippe Defraigne

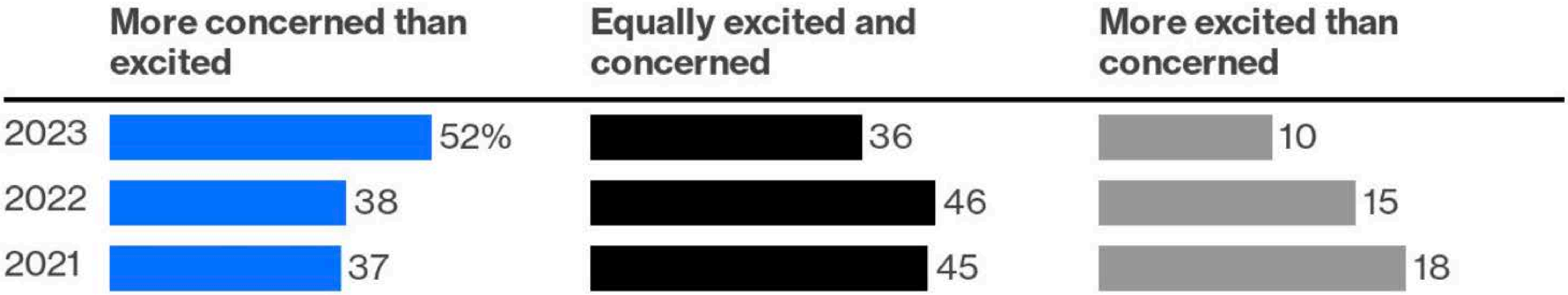
CRC | 3 Dec 2024

# Why regulate AI?



## As AI Becomes More Pervasive, So Does Concern About It

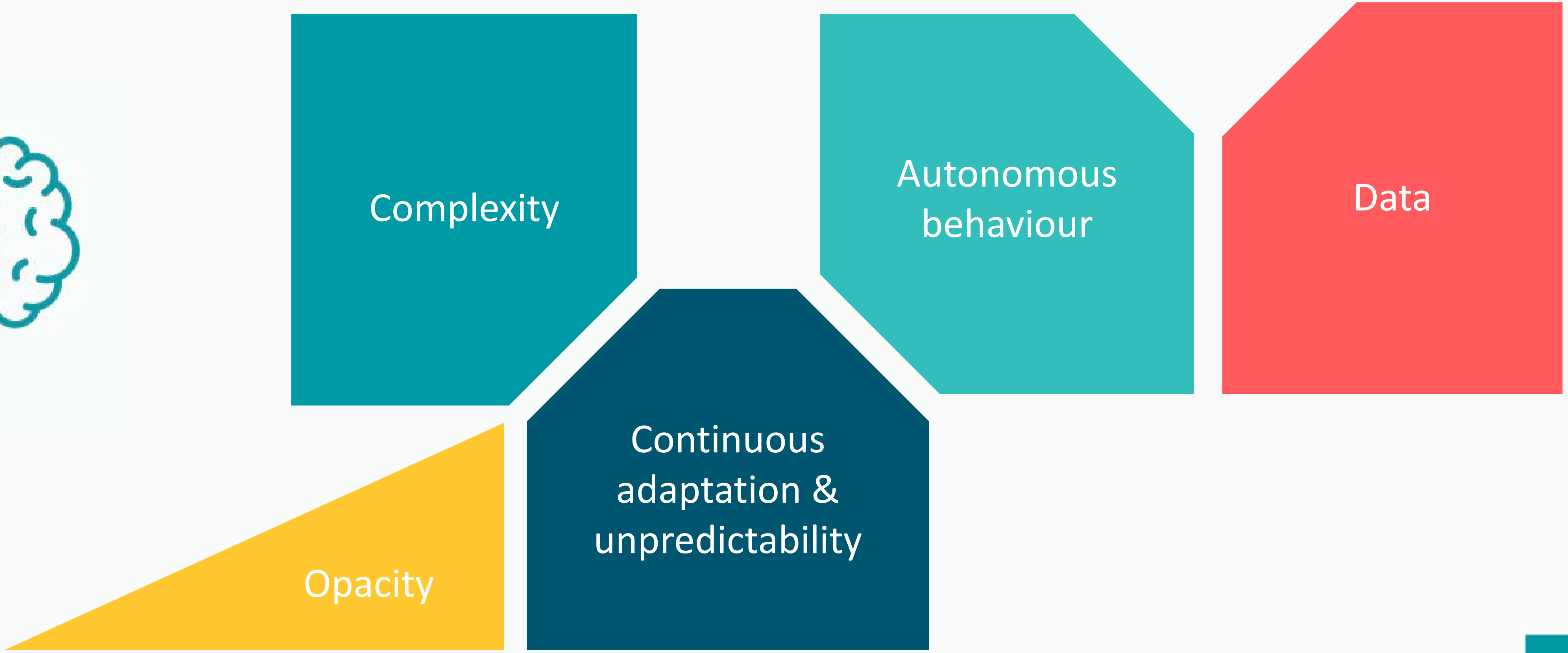
Last year, Americans started to worry a lot more about the increased use of artificial intelligence in their daily lives



Source: Pew Research Center

Bloomberg Opinion

# Specific characteristics of AI & related challenges



Complexity

Autonomous behaviour

Data

Continuous adaptation & unpredictability

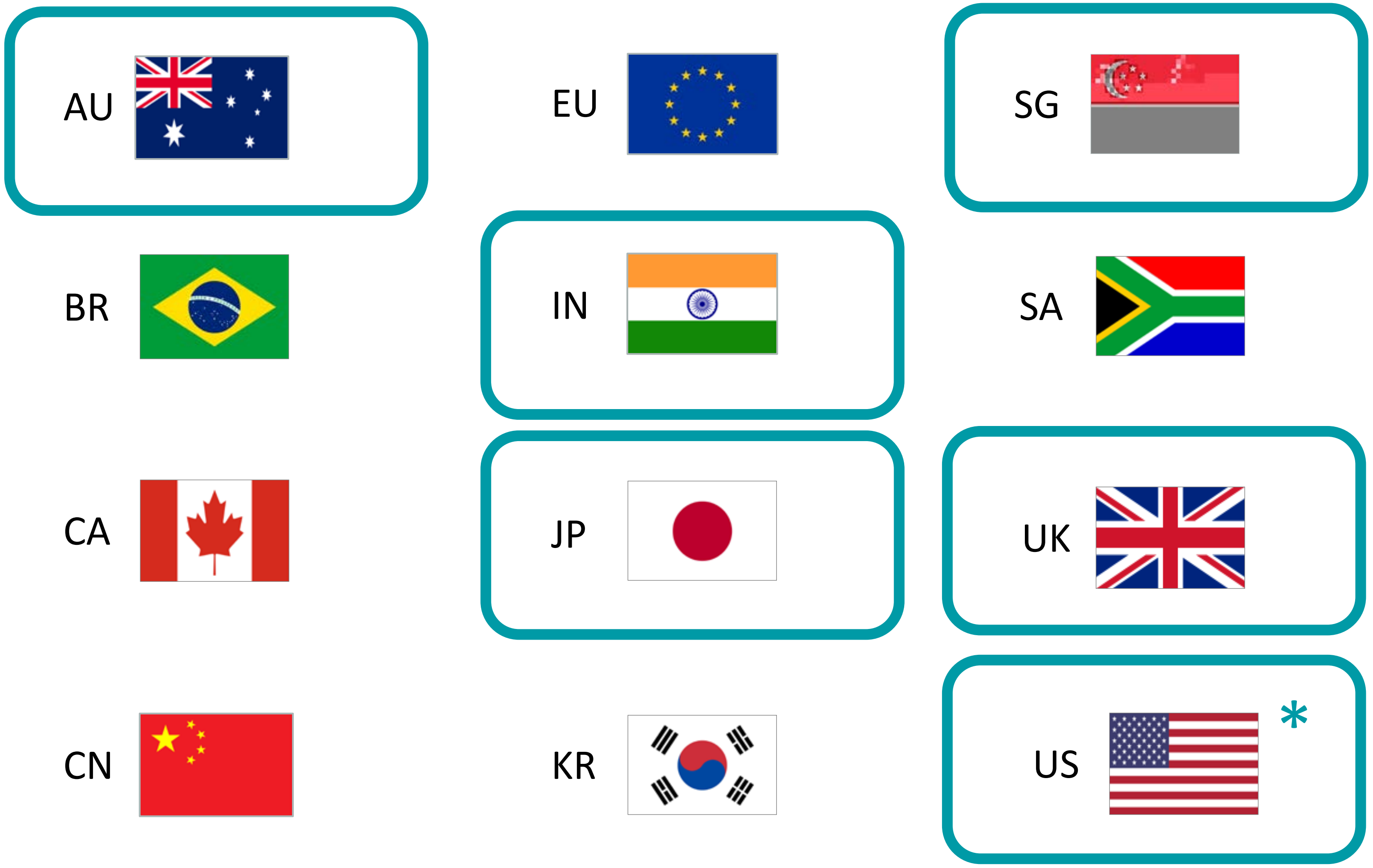
Opacity

# Regulatory approaches to AI

# Scope

- AU
- BR
- CA
- CN
- EU
- IN
- JP
- KR
- SG
- SA
- UK
- US

# Principles-based approach (responsible use)



AU

BR

CA

CN

EU

IN

JP

KR

SG

SA

UK

US *

# Principles-based approach (responsible use)

| | | |
|---|---|---|
| **AU** | EU | **SG** |
| BR | **IN** | SA |
| CA | **JP** | **UK** |
| CN | KR | **US** * |

+

OECD

G7 2023 HIROSHIMA SUMMIT

Trade and Technology Council

# UK approach to AI

- March 2023 - UK Department for Science, Innovation and Technology (DSIT) published its AI white paper, detailing the government’s approach to AI.

# UK approach to AI

- a non-legislative framework for AI
- five cross-sectoral principles:
  - Safety, security and robustness
  - Transparency and Explainability
  - Fairness
  - Accountability and governance
  - Contestability and redress

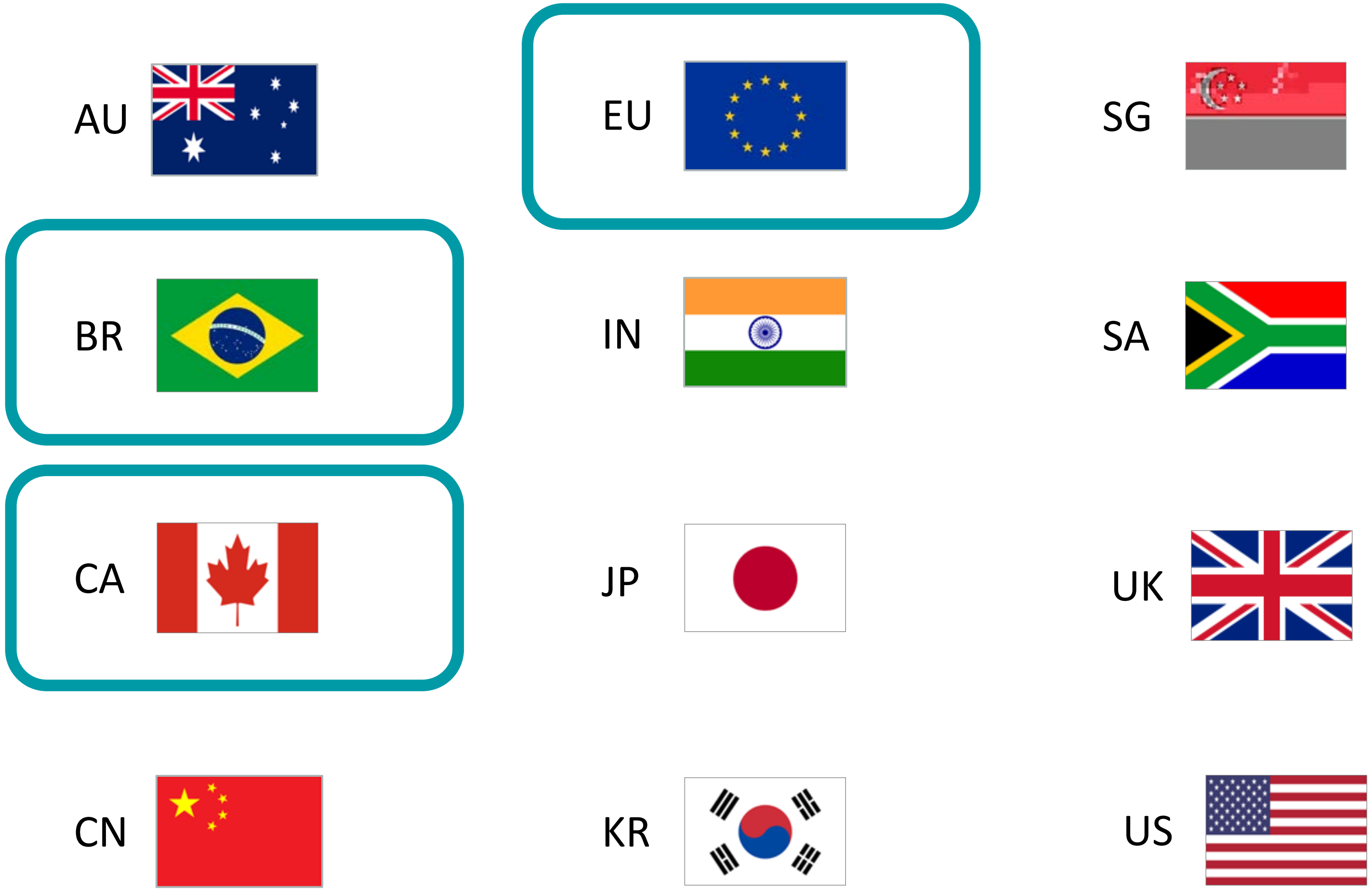
# UK approach to AI

- Digital Regulation Cooperation Forum (DRCF)
- AI and Digital Hub, a pilot scheme for a brand-new advisory service to support innovation run by expert regulators including Ofcom, CMA, FCA and ICO

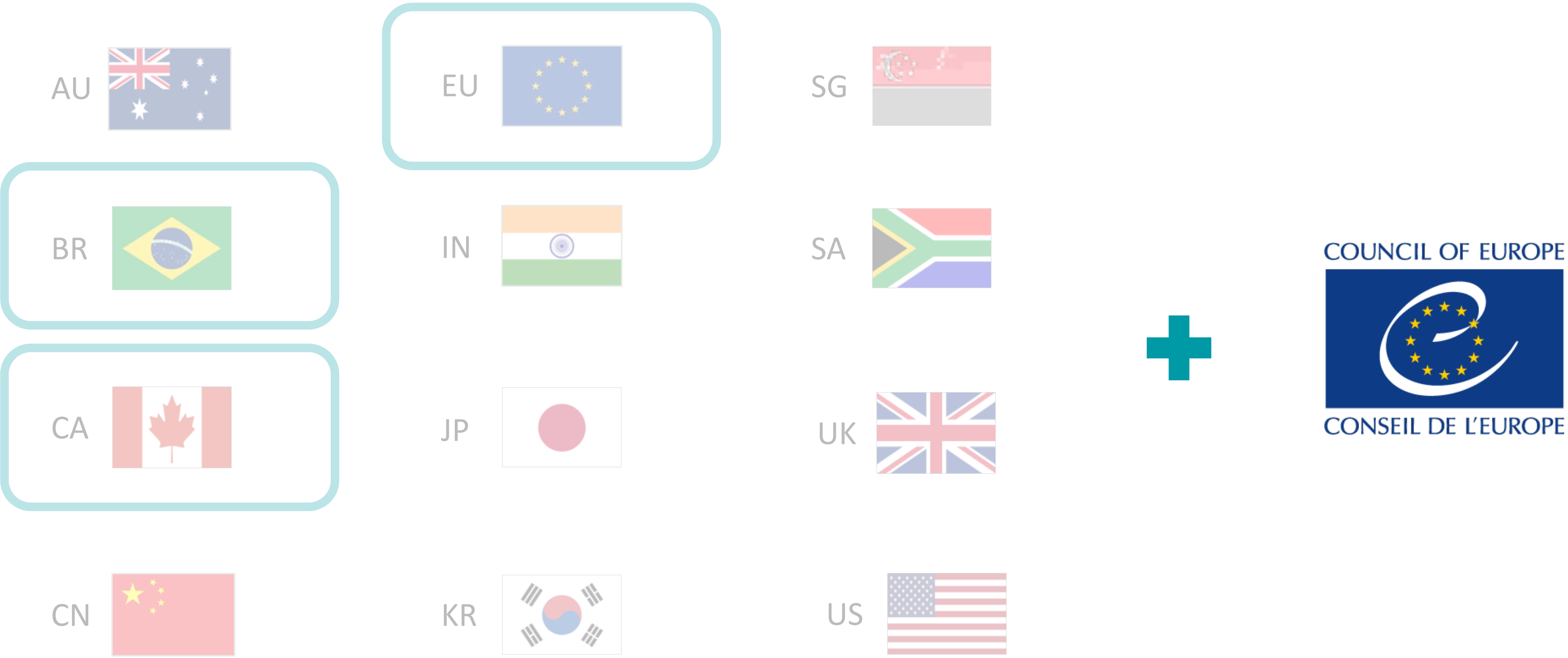
# UK approach to AI

- The UK light-touch approach to AI stands in contrast to the EU regulatory approach!

# Risk-based approach



# Risk-based approach



AU

EU

SG

BR

IN

SA

CA

JP

UK

CN

KR

US

# Technology-specific approach

AU

BR

CA

CN

EU

IN

JP

KR

SG

SA

UK

US

# Back to Europe and the 2016 GDPR

# GDPR & AI

automated decision-making and profiling

(article 22)

the use of biometric data for remote biometric identification

(article 9)

# Transparency of algorithms

# Case study: Turkcell credit scoring service to banks

Based on over 600 parameters collected by the phone and reconciled with credit history

# GDPR - Profiling

Profiling “is often used

1. to make **predictions about people**,
2. using **data** from **various sources**
3. **to infer something about an individual,**
4. based on the **qualities of others** who appear **statistically similar**”. (WP29)

CULLEN INTERNATIONAL

# GDPR - Profiling

Examples:

Profiling may be used to “**analyse or predict**” that individual's **performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.** (GDPR)

# Automated individual decision-making, including profiling

## GDPR - Article 22

- The data subject shall have **the right not to be subject to a decision based solely on automated processing**, including **profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her.
- GDPR foresees some common-sense exceptions
- Art 29 WP adopted guidelines on February 6, 2018.

# Automated individual decision-making

## Safeguards

The data controller must ensure individuals' right to:

- **obtain human intervention**;
- express their opinion; and
- **contest the decision.**

# Automated individual decision-making

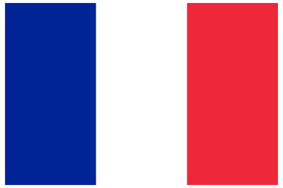
Under the GDPR (Art 22), controllers must also perform a **data protection impact assessment** (DPIA) before using automated decision-making processes.

## AI and fully automated process: the case for Transparency

Transparency of AI is an issue not limited to privacy!

- Competition Law cases involving AI-based decisions (‘intentionality’/ ’good faith’)
- Financial markets regulators investigating asset price volatility

# France - Transparency of algorithms



President Macron in March 2018 presenting France’s AI strategy. We should …

**increase transparency and loyalty**

- Make government algorithms transparent
- **Search for any bias**
- **Not grant them** the **monopoly of decision** making
- Commit to **complement** them **with human decision**

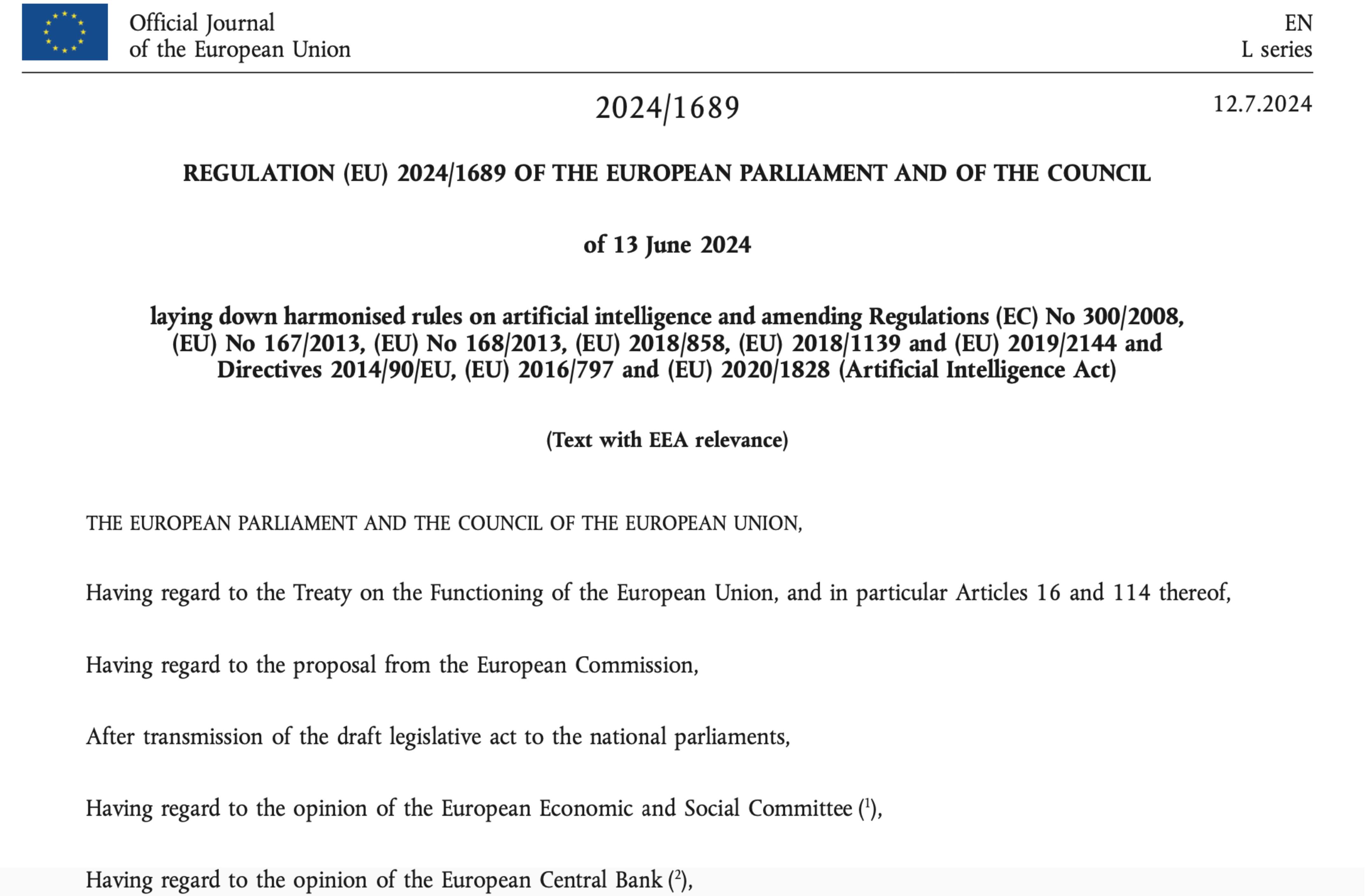
# France - Loyalty of algorithms

## President Macron (cont'd)

- …the need to make the **algorithm more democratic** and therefore to be sure of its **loyalty** and of its perfect **transparency**..
- ..so that **a debate can take place on the rules**..otherwise, we **delegate** to the algorithm the choice between **democratic priorities**

# The EU Artificial Intelligence Act

“The ~~proposed~~ legal framework doesn't look at AI technology itself. Instead, it looks at how AI is used, and what for.”



Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

# REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

## of 13 June 2024

## laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

**(Text with EEA relevance)**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee [1],

Having regard to the opinion of the European Central Bank [2],

# What is AI?

AI is defined through a list of techniques*

- machine learning
- logic- and knowledge-based approaches
- statistical approaches

*Annex 1; The Commission could adapt the list of techniques “in line with new technological developments”.

# What is an AI system?

‘AI system‘ is a machine-based system designed to operate with varying levels of **autonomy** and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, **infers**, from the **input** it receives, how to generate **outputs** such as predictions, content, recommendations, or decisions that can influence physical or virtual environments (Art 3.1 AIA)

# OECD definition of AI

- The OECD defines an *Artificial Intelligence (AI) System* as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.

(Guidelines for multinational enterprises – see here)

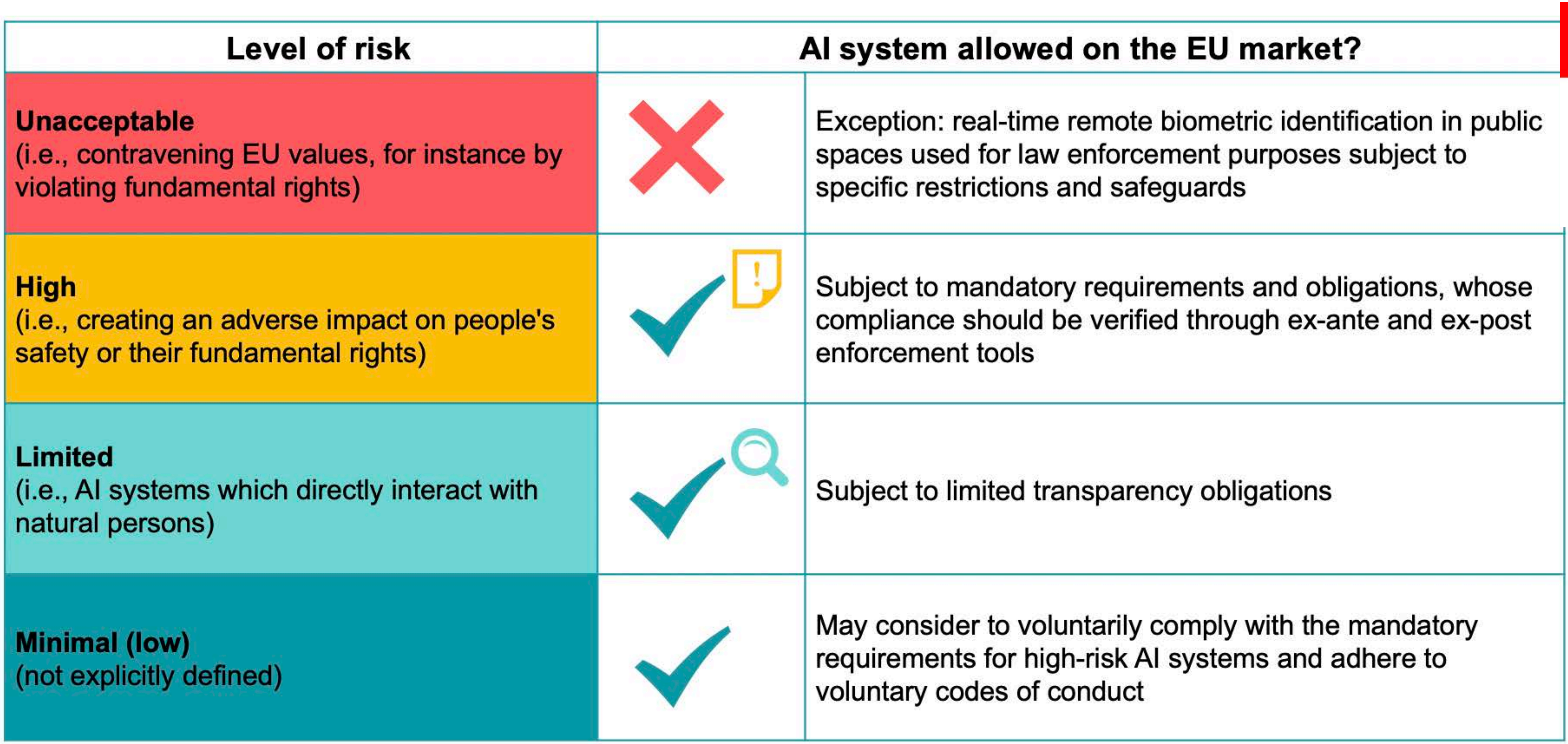
# Outside the scope

Excluded from definition of AI systems:

- exclusively used for **national security purposes**
- developed solely for **scientific research** and development
- **tested before being put on the market** (except if tested in real-world conditions)
- Also, exemptions for free and open-source AI systems and GPAI models across the text.

RISK
MAXIMUM
HIGH
MEDIUM
LOW
MINIMUM

# Artificial Intelligence Act (AIA)



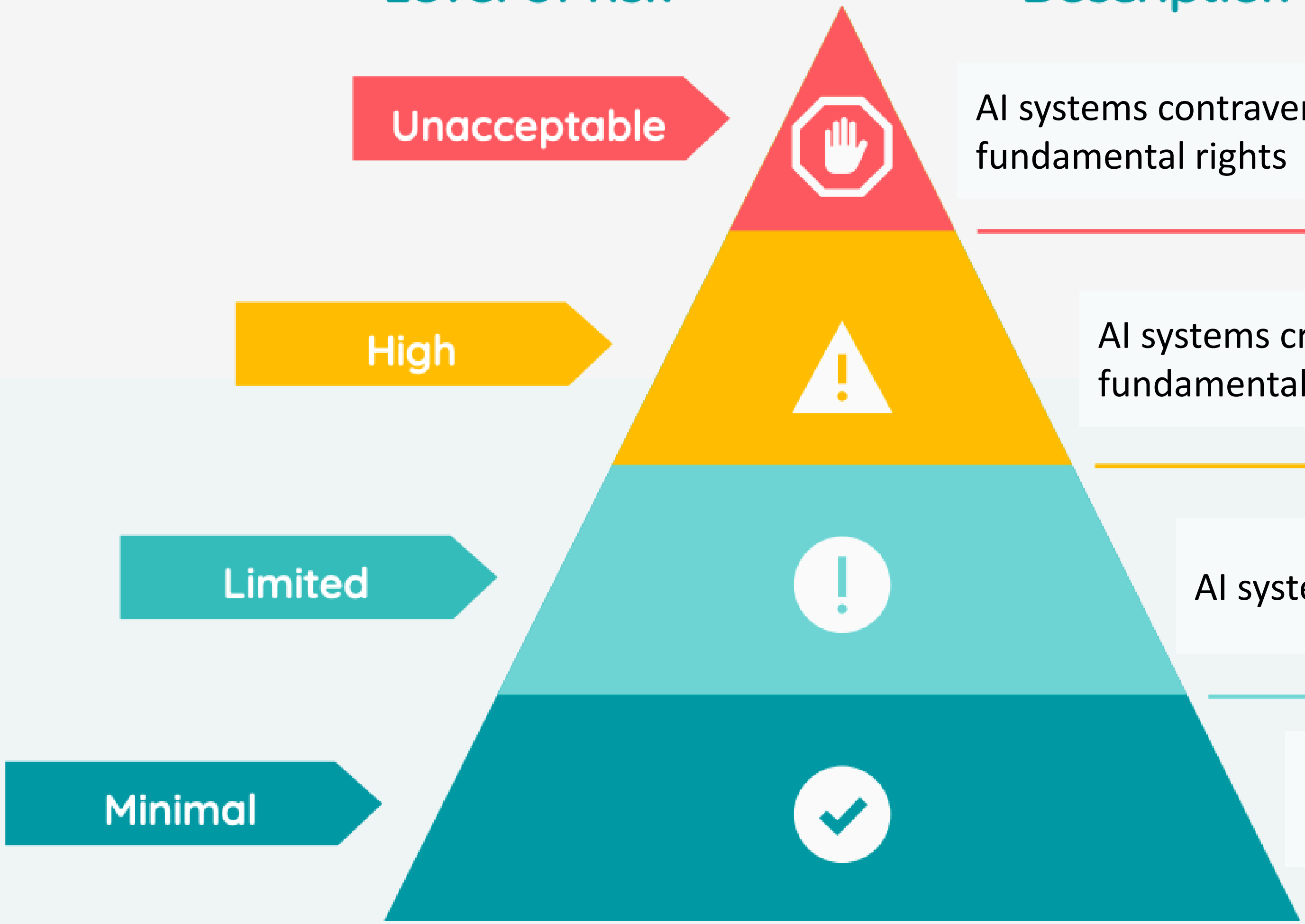
| Level of risk | AI system allowed on the EU market? | |
|---|---|---|
| **Unacceptable**<br>(i.e., contravening EU values, for instance by violating fundamental rights) | ✗ | Exception: real-time remote biometric identification in public spaces used for law enforcement purposes subject to specific restrictions and safeguards |
| **High**<br>(i.e., creating an adverse impact on people's safety or their fundamental rights) | ✓ ! | Subject to mandatory requirements and obligations, whose compliance should be verified through ex-ante and ex-post enforcement tools |
| **Limited**<br>(i.e., AI systems which directly interact with natural persons) | ✓ 🔍 | Subject to limited transparency obligations |
| **Minimal (low)**<br>(not explicitly defined) | ✓ | May consider to voluntarily comply with the mandatory requirements for high-risk AI systems and adhere to voluntary codes of conduct |

© Cullen International

TARGET

CULLEN INTERNATIONAL

# A risk-based approach shapes the draft AIA



| Level of risk | Description |
|---|---|
| Unacceptable | AI systems contravening EU values, for instance by violating fundamental rights |
| High | AI systems creating an adverse impact on people’s safety or fundamental rights |
| Limited | AI systems directly interacting with natural persons |
| Minimal | Other AI systems |

# Unacceptable

# AIA - Prohibited AI practices

- AI systems that exploit any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, to materially distort a person’s behaviour;

# AIA - Prohibited AI practices

- AI systems used by public authorities for general purpose **<u>social scoring</u>** with the social score leading to detrimental or unfavourable treatment.
- So, evaluation or classification of the trustworthiness of natural persons

# High risk

# AIA - High-risk AI systems

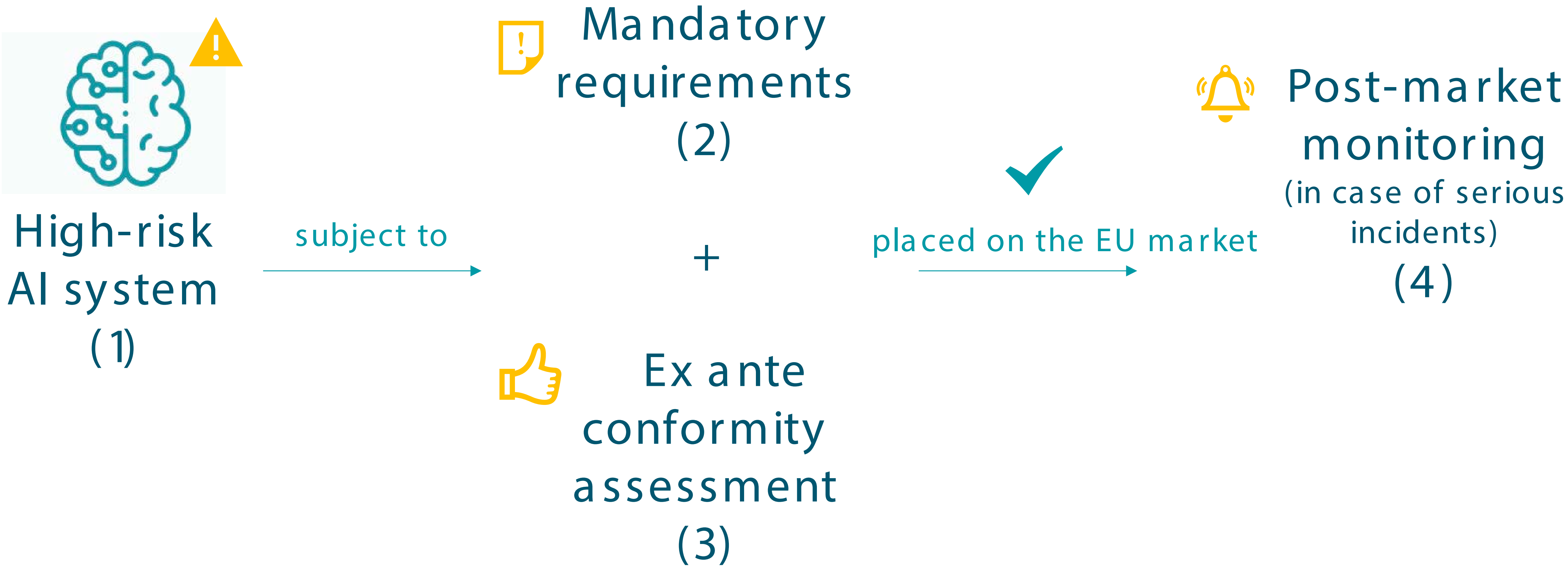
High-risk AI systems = with a significant harmful impact on the

- health,
- safety,
- fundamental rights of persons …(Recital 27)

# AIA - High-risk AI systems

- Stand-alone AI systems posing a high risk of harm to the health and safety or the fundamental rights of persons.
- Such AI systems include:
  - Biometric identification and categorisation of natural persons
  - operation of critical infrastructure road traffic, water, gas, heating and electricity
  - education and vocational training (e.g., exam scoring),.
  - See Annex III for full list

# High-risk AI systems*



High-risk AI system (1)

subject to

Mandatory requirements (2)

+

Ex ante conformity assessment (3)

placed on the EU market

Post-market monitoring (in case of serious incidents) (4)

*EP envisages:

- a fundamental rights impact assessment
- a separate self-assessment for certain high-risk use cases

# High-risk AI systems ⚠ (1) Types

1. Safety components of products or products themselves, falling within the scope of one of 19 specified pieces of EU harmonised legislation

e.g. machinery, toys, lifts, medical devices, motor vehicles, agricultural/forestry vehicles

ℹ Annex II

2. Stand-alone AI systems deployed and used in 8* pre-defined areas

e.g. traffic management systems, exam scoring

ℹ Annex III

*EP and Council introduce/ remove the use cases

RISK
Safe
Risk

# AIA - High-risk AI systems

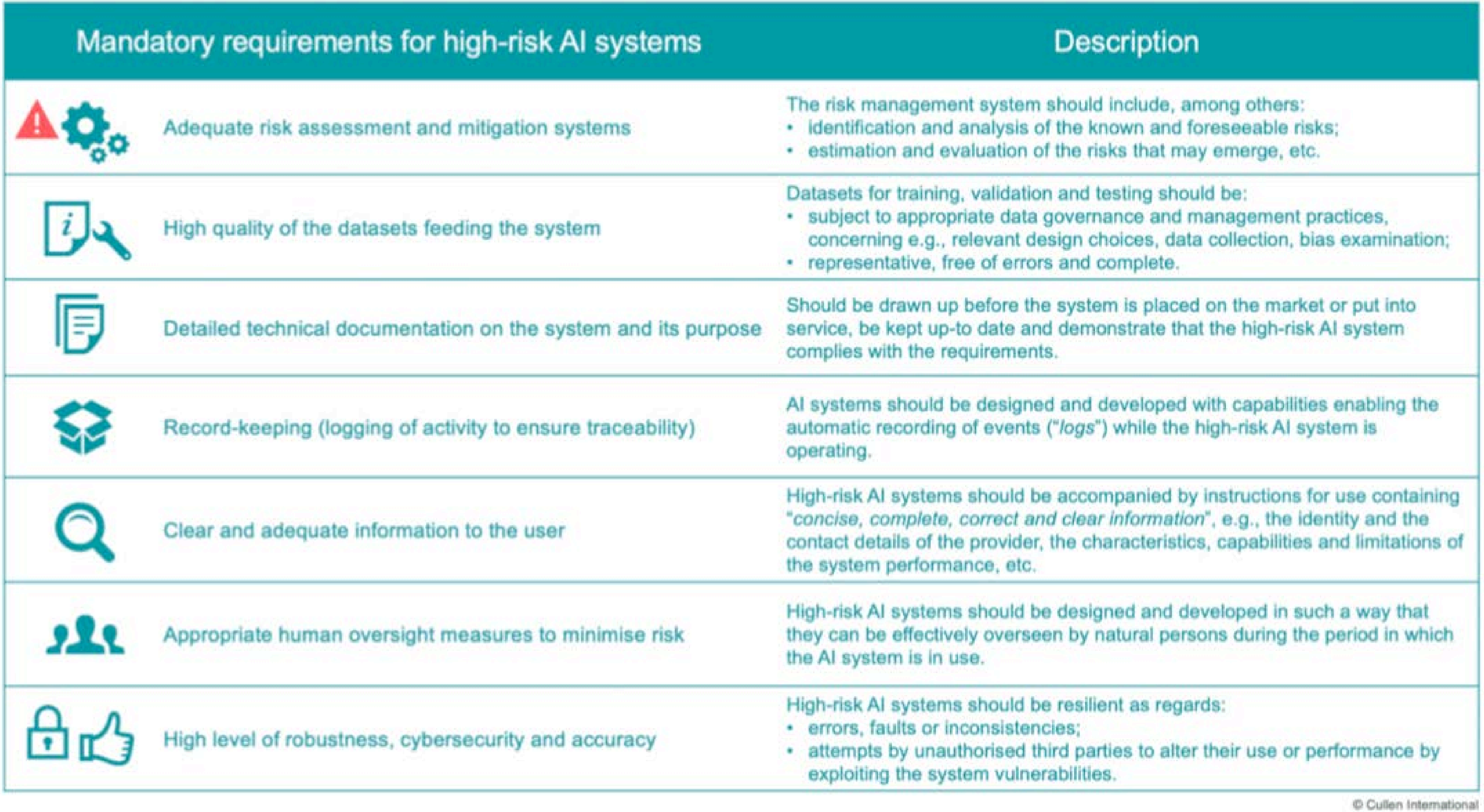
Classification of AI systems as high-risk to health or fundamental rights would depend on intended purpose, considering:

1. the severity of the possible harm and
2. its probability of occurrence.

# Mandatory requirements for High-risk AI systems

TARGET

Requirements for high-risk AI in the proposed AIA (Cullen International)



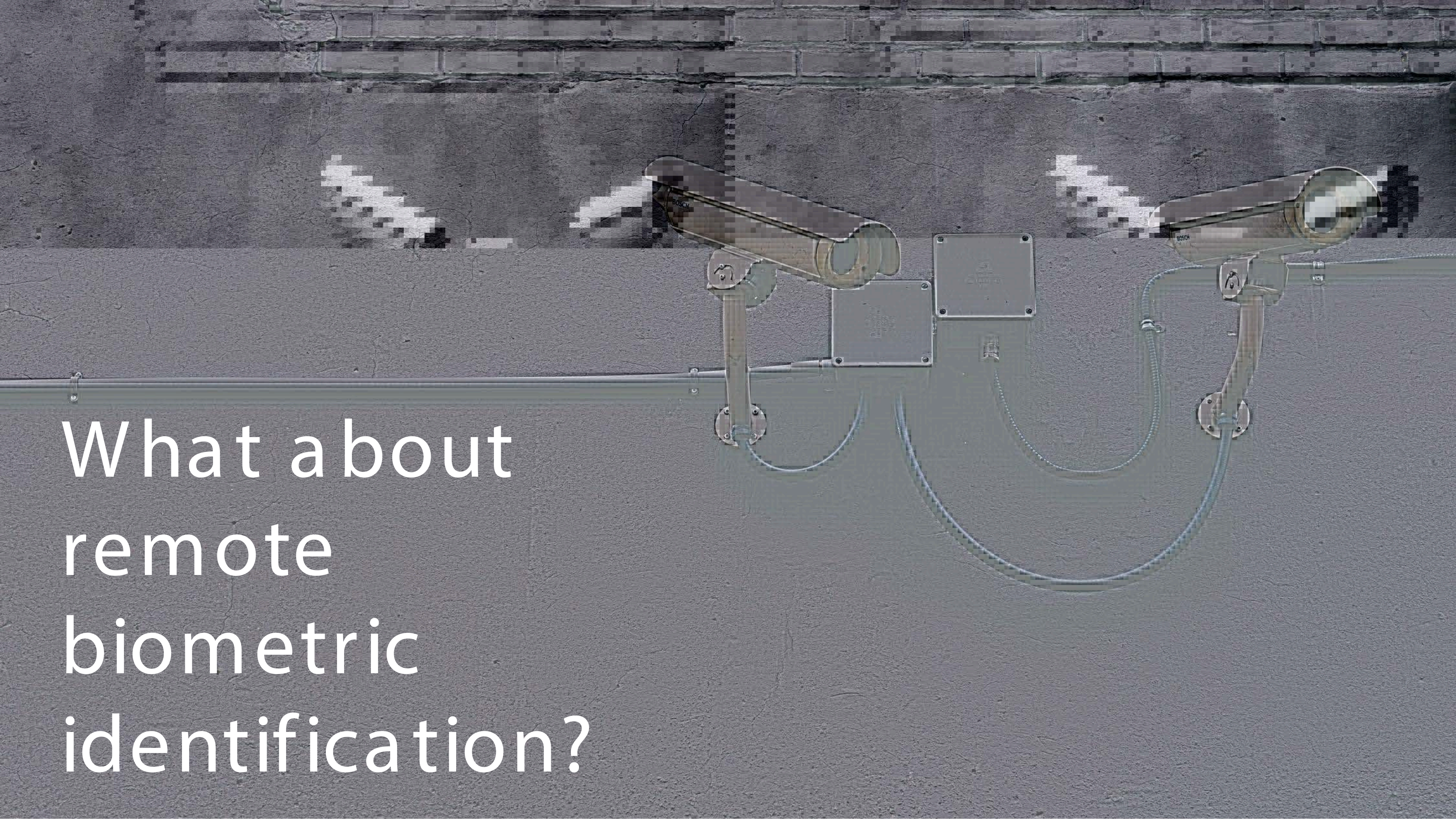
| Mandatory requirements for high-risk AI systems | Description |
|---|---|
| Adequate risk assessment and mitigation systems | The risk management system should include, among others:<br>• identification and analysis of the known and foreseeable risks;<br>• estimation and evaluation of the risks that may emerge, etc. |
| High quality of the datasets feeding the system | Datasets for training, validation and testing should be:<br>• subject to appropriate data governance and management practices, concerning e.g., relevant design choices, data collection, bias examination;<br>• representative, free of errors and complete. |
| Detailed technical documentation on the system and its purpose | Should be drawn up before the system is placed on the market or put into service, be kept up-to date and demonstrate that the high-risk AI system complies with the requirements. |
| Record-keeping (logging of activity to ensure traceability) | AI systems should be designed and developed with capabilities enabling the automatic recording of events ("*logs*") while the high-risk AI system is operating. |
| Clear and adequate information to the user | High-risk AI systems should be accompanied by instructions for use containing "*concise, complete, correct and clear information*", e.g., the identity and the contact details of the provider, the characteristics, capabilities and limitations of the system performance, etc. |
| Appropriate human oversight measures to minimise risk | High-risk AI systems should be designed and developed in such a way that they can be effectively overseen by natural persons during the period in which the AI system is in use. |
| High level of robustness, cybersecurity and accuracy | High-risk AI systems should be resilient as regards:<br>• errors, faults or inconsistencies;<br>• attempts by unauthorised third parties to alter their use or performance by exploiting the system vulnerabilities. |

© Cullen International

CULLEN INTERNATIONAL

# AIA – Incident reporting

- AI providers to inform national competent authorities about serious incidents or malfunctioning that constitute a breach of fundamental rights obligations and withdrawals of AI systems from the market.



# What about remote biometric identification?

# Remote biometric identification (RBI)

## Always considered high-risk AI system ⚠

### Restrictions ✗

‘real time’ RBI systems in publicly accessible spaces for the purpose of law enforcement: prohibited in principle, with a few exceptions:

- the targeted search for potential crime victims, including missing children;
- the prevention of a threat to the life of people or a terrorist attack; or
- the detection, localisation, identification or prosecution of a perpetrator or suspect of a criminal offence*

*Article 2 (2) of Council Framework Decision 2002/584/JHA

### Safeguards

Prior judicial authorisation

Mandatory requirements

Ex ante conformity assessment by an independent body

+

EU countries may authorise the use of such systems fully or partially in their national laws

# High-risk AI systems ⚠ Who would be subject to AIA? (4)

## Addressees

Authorised representative if outside the EU

Exception: public authorities in a third country or international organisations

Private actors (natural or legal person)

&

Public actors (national or EU public authority, agency or other body)

Inside and outside the EU as long as the AI system is:

- placed on the EU market; or
- its use affects people located in the EU.

## Roles & obligations

### Provider

Ensure overall compliance of high-risk AI systems with AIA's requirements:

- Mandatory requirements
- Ex-ante conformity assessment
- EU declaration of conformity
- CE marking of conformity
- Post-market monitoring system

### Importer

### Distributor

Ensure that the high-risk AI system has been brought into conformity by the provider before making it avaiålable on the market.

### User

Use high-risk AI systems according to the accompanying instructions of use.

Could be considered providers in several cases (e.g. if they modify the intended purpose of a high-risk AI system)

# Limited risk

CULLEN INTERNATIONAL

# AIA – AI systems presenting a limited risk

- Providers of AI systems intended to interact with natural persons (e.g., chatbots) would be s.t. transparency obligations
- Users would have to be notified that they are interacting with such AI systems.
- These would include:
  - emotion recognition systems;
  - biometric categorisation systems;
  - AI systems that generate or manipulate image, audio or video content (e.g., deep fakes).

# Minimal risk

CULLEN
INTERNATIONAL

# AIA – AI systems presenting a minimal risk

- Most AI systems currently used in the EU fall into this category (e.g., AI-enabled video games or spam filters).
- Voluntarily, providers of those systems would be able to choose to apply the mandatory requirements for high-risk AI systems or adhere to voluntary codes of conduct.

# General-Purpose AI

## GPAI definition

GPAI models are defined as those AI models

- displaying “significant generality”
- able to perform a variety of tasks
- integrated into different downstream AI systems

# GPAI models presenting systemic risks: designation

GPAI models presenting systemic risks (high-impact capabilities) will be designated by the Commission following either

- a fast threshold-based designation procedure
- an ad-hoc designation procedure

# GPAI models presenting systemic risks: designation

- GPAI models are presumed to have high-impact capabilities if the computational resources used for their training exceed 10^25 floating-point operations.
- A floating-point operation is a single calculation, such as the multiplication of two numbers. A modern PlayStation or Xbox gaming console would have to be playing at full capacity for about 30,000 years to reach an equivalent threshold.

# Obligations fot all GPAI models

- Keeping up-to-date technical documentation of the model (annex IXa)
- Making additional documentation available to other providers who want to integrate the model into their AI systems (annex IXb)
- Establishing a policy to respect EU copyright law (recital 60i recalls that if rights holders reserved the rights for text and data mining, providers of GPAI models would need authorisation from them)
- Publishing a comprehensive summary detailing the content used for training the model, “taking into due account of the need to protect trade secrets and confidential business information” (recital 60k)

# GPAI models presenting systemic risks: obligations

- Performing model evaluation, including by conducting adversarial testing (red/blue teams) of the model to identify and mitigate risks
- Conducting a systemic risk assessment and taking risk mitigation measures
- Ensuring an adequate level of cybersecurity for the model, including its physical infrastructure
- Reporting serious incidents to the AI Office

# GPAI and AI Office

- GPAI models will be supervised through a pan European governance system centralised around the Commission AI Office

# Fines

# Non-compliance & penalties

| Infringement | Penalty<br>Administrative fines OR % of worldwide annual turnover, whichever is higher | |
|---|---|---|
| Non-compliance with the prohibition of AI systems posing an unacceptable risk* or with the mandatory requirements for high-risk AI systems | €30m | 6% |
| Non-compliance with any requirements or obligations under the regulation | €20m | 4% |
| Provision of incorrect, incomplete or misleading information to notified bodies and national competent authorities | €10m | 2% |

Up to

Similar to the GDPR regime

*EP envisages up to €40m or 7% of the worldwide annual turnover, whichever is higher

# Enforcement

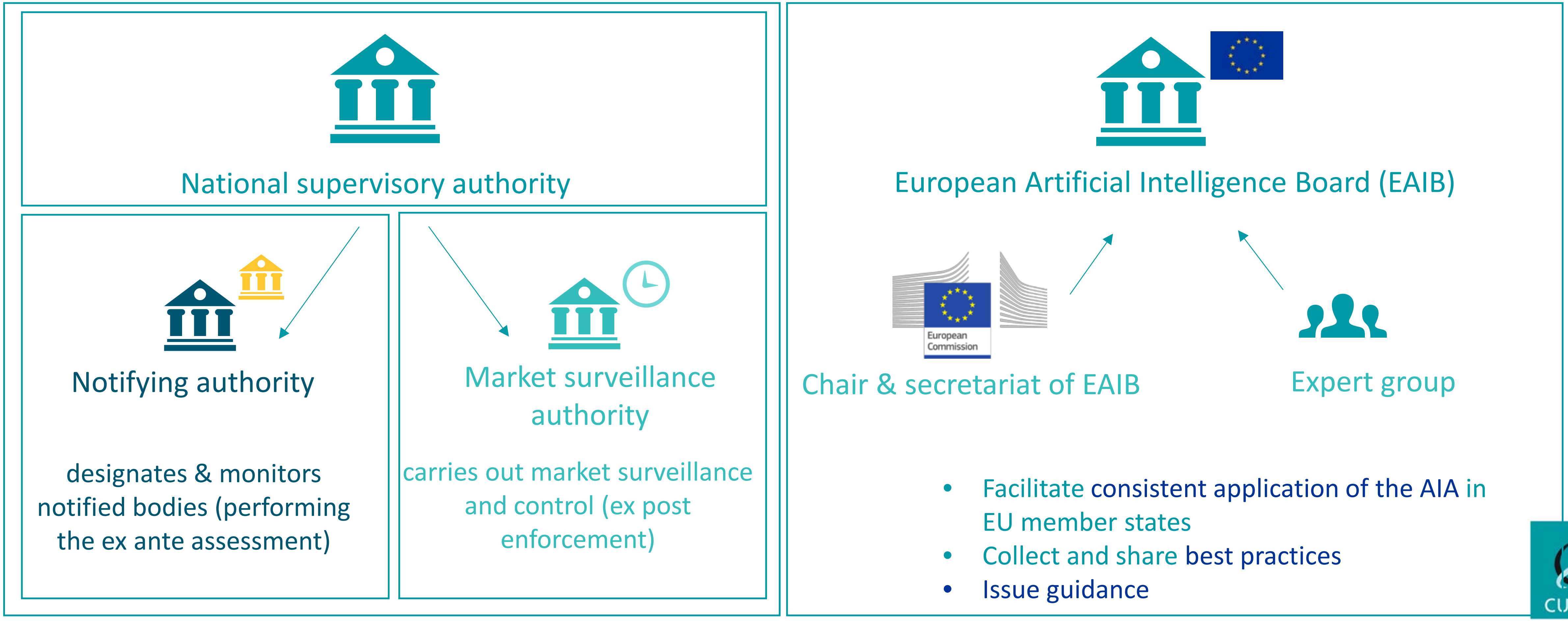
# Governance & enforcement

## National level

Key for implementation and enforcement

## EU level

Coordination and guidance



National supervisory authority

Notifying authority

designates & monitors notified bodies (performing the ex ante assessment)

Market surveillance authority

carries out market surveillance and control (ex post enforcement)

European Artificial Intelligence Board (EAIB)

Chair & secretariat of EAIB

Expert group

- Facilitate consistent application of the AIA in EU member states
- Collect and share best practices
- Issue guidance

# AI Office

- European Commission AI Office with sweeping powers in AIA governance
- The AI Office will have ample investigatory and enforcement powers over GPAI models, for example, to:
- request access to the model through application programming interfaces (APIs) or other means such as source codes, to evaluate it; and
- impose fines of up to 3% of the annual worldwide turnover (or €15m), whichever is higher (in contrast with the highest fine under the AIA of 7% (or €30m) for violations of the banned AI practices).
- Regarding the European Artificial Intelligence Board (EAIB), the tasks of this advisory body would be extended. For example, it could deliver opinions to the Commission regarding GPAI models.
- At national level, EU countries will have flexibility to appoint more than one notifying authority and MSA. In line with the Commission proposal, MSAs will be responsible for carrying out market surveillance and control of AI systems (including high-risk AI systems) placed on the EU market.

CULLEN
INTERNATIONAL

# Thank you!

phil@cullen-international.com