



AI  
AI & Partners

# **Artificial Intelligence Act**

APRIL 2023

**For Public Use**



# The *European Artificial Intelligence Act* summarised

Where do you see the EU AI Act impacting you?

The Proposal for a regulation lays down harmonised rules on artificial intelligence.



## What does it focus on?

- Human centered Risk-based approach
- Classification of AI systems



## Who does it apply to?

- Providers, Users, Importers and Distributors of AI systems inside of the EU



## When will it apply?

- Scheduled to take effect from January 2024



## Why should I care?

- Clients might already have AI systems in place
- Non-compliance can lead to fees up to 30.000.000€ or 6% of turnover



## What can I do?

- Inform clients about the topic
- AI & Partners with Trustworthy AI has the necessary competence



On April 21, 2021, the European Commission proposed the first legal framework on AI ever, that addressed the risks of AI and positions the European Union to play a key role globally. The proposal is comprehensive, so this document provides an **overview** for you.



# The Goal of the European Artificial Intelligence Act

How do you take ethical implications of AI use cases into account

The Proposal sets down a legislative framework for dealing with AI in the future - with the goal of driving innovation and mitigating risks.

## EU AI Act is about....

Emphasising the **ethical application of AI**, instilling European values while improving transparency.

Establishing a process and roles to **enforce quality** at launch and throughout the life cycle

Fostering collaboration and a level **playing field** between EU member states and protecting fundamental rights of EU citizens in the age of AI.



## Penalties

Infringements can lead up to **€30M or 6% of global annual turnover** when violating Art. 5 or Art. 10.

Other non-compliance with requirements may result in a fine of **€20M or 4%** of global annual turnover.

## How it intends to achieve that....

Incorporating a single standard **across the EU** to prevent fragmentation, enforced through **Conformity Declarations** and the obligation for a **CE marking**.

Providing **legal certainty** that encourages innovation and investment into AI by creating AI Regulatory Sandboxes.

Enabling National competent authorities as control instances. These instances will update a **EU database** for high-risk AI practices and systems.

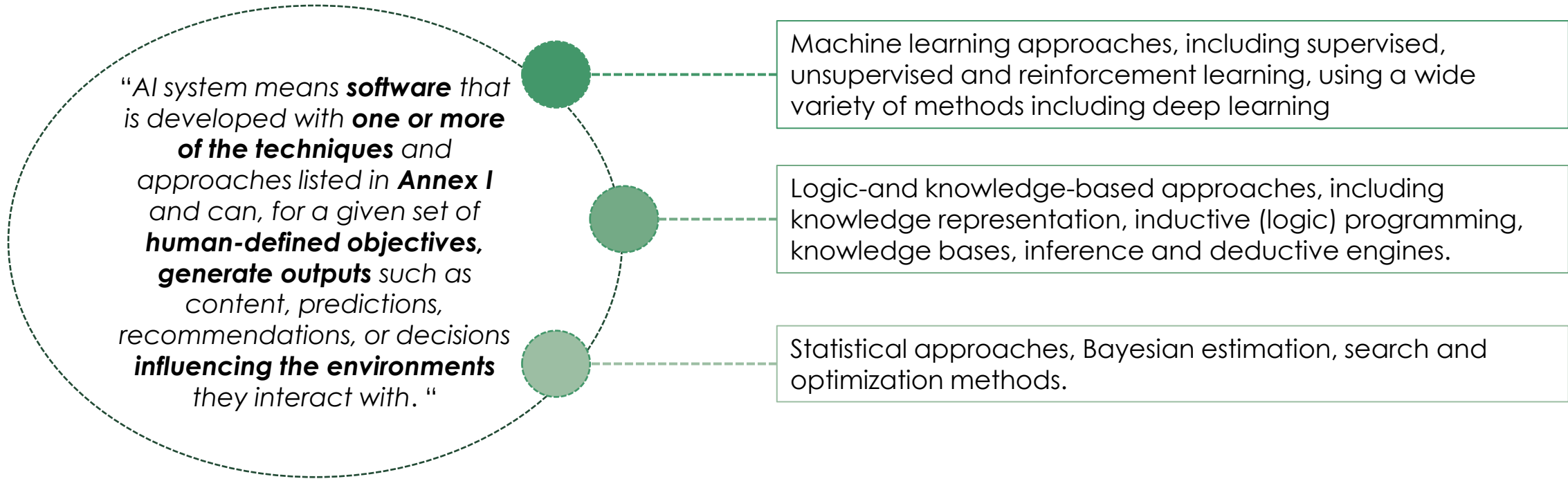
Infringements can lead up to **€30M or 6% of global annual turnover** when violating Art. 5 or Art. 10.



# A Wide Definition of AI

What model do you have that would be considered as AI?

The European Artificial Intelligence Act considers not only machine learning, but expert systems and statistical models long in place.



<b>Comprehensive</b>	<b>Future proof</b>	<b>Legally secure</b>
cover all current and future AI including machine learning, deep learning as well as hybrid systems	by focusing more on the use cases than on AI technology itself.	neutral as possible in regards to technical details in order to cover techniques which are unknown.



# Scope of the European Artificial Intelligence Act

How are you affected?  
As a provider,  
distributor, importer or  
user?

The Proposal focuses on high-risk AI systems being provided to/used in the European Union.

## Requirements/obligations of the European AI Act

### Applies to Entities

- Bodies inside and outside the EU if their AI system is running or affecting people in the EU.
- Providers/Importers/Distributors provisioning AI within the EU.
- Users of AI systems within the EU.
- Providers and users located in a third country but where the output produced by the AI system is used in the Union.

### Entities Out-of-Scope

- Public authorities in a third country nor international organizations using AI systems in the framework of international agreements for law enforcement and judicial cooperation with the Union or with one or more Member States.
- Military institutions.
- Purely private, non-commercial use.



# Overview of artificial intelligence systems

Have you taken stock of your current AI systems and their degree of risk?

The Proposal uses a risk-based approach to differentiate between four types of AI systems based on their potential for hazards and risk.

<b>Unacceptable Risk Artificial Intelligence Systems (Art. 5)</b>	<b>High-Risk Artificial Intelligence Systems (Art. 6)</b>	<b>AI with specific transparency obligations (Art. 52)</b>	<b>Minimal or no Risk Artificial Intelligence Systems</b>
<p>Prohibited:</p> <ul style="list-style-type: none"><li>• Manipulation of human behaviour, opinions and decisions.</li><li>• Classification of people based on their social behaviour.</li><li>• Real-time remote biometric identification, except for certain exceptions with special express authorization.</li></ul>	<p>Permitted subject to compliance with AI requirements ex-ante conformity assessment*.</p> <ul style="list-style-type: none"><li>• Main focus of the regulation (Annex III).</li><li>• Common schemes with those already subject to a harmonized EU standard.</li><li>• Additional list to be reviewed every year by the EAIB (Art. 84).</li></ul>	<p>Permitted but subject to information/transparency obligations</p> <ul style="list-style-type: none"><li>• Interaction with humans.</li><li>• Use to detect emotions or determine categories based on biometric data.</li><li>• Generation of manipulate content.</li></ul>	<p>Permitted without restrictions</p>
<b>Example: Social Scoring</b>	<b>Example: Recruitment</b>	<b>Example: Impersonation (Bots)</b>	<b>Example: predictive Maintenance</b>

\*Exceptions are High-risk AI system developed or used for military purposes. For HRAIS which are regulated by one of the following, only Article 84 should apply. Regulation (EC) 300/2008; Regulation (EU) No 167/2013; Regulation (EU) No 168/2013; Directive 2014/90/EU; Directive (EU) 2016/797, Regulation (EU) 2018/858; Regulation (EU) 2018/1139; Regulation (EU) 2019/2144



# Unacceptable Risk AI Systems (Art. 5)

Do you provide AI systems that would be considered unacceptable risks?

Applications of AI that pose an unacceptable risk are prohibited.

**1. Subliminal manipulation** resulting in physical/psychological harm

**Example:** To push truck drivers to drive longer than healthy and safe, an inaudible sound 1 is played in their cabin. AI is used to find the frequency maximizing this effect on drivers.

**2. Exploitation of children, mentally disabled or vulnerable persons** resulting in physical/psychological harm

**Example:** : A toy with an integrated voice assistant leads children to engage in dangerous behaviour in the guise of a learning game.

**3. General purpose social scoring**

**Example:** An AI system calculates the credit range for people based on insignificant or irrelevant social "misbehaviour".

**4. Real-time remote biometric identification** for law enforcement purposes in publicly accessible spaces\*

**Example:** To find a low-level criminal, all public available cameras scan each face which appears in the view of the camera and checks it against a database in real time.

\*with exceptions



# High-Risk AI Systems (Art. 6)

Which AI systems do you provide/use, which may be considered high-risk?

High-risk AI is defined both by general characteristics and specifically targeted applications.

## High-Risk AI Systems (Art. 6)

- AI systems used as safety component of a product or stand-alone product.
- Product or AI system covered by the Union harmonization legislation listed in Annex II (e.g. Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending).
- If putting into service or placing on the market requires a third-party conformity assessment.

## Specific Fields of AI deemed High-Risk (Annex III)

- List includes the following:
  - Biometric identification and categorization of natural persons
  - Management and operation of critical infrastructure
  - Education and vocational training
  - Employment, workers management and access to self-employment
  - Access to and enjoyment of essential private services and public services and benefits
  - Law enforcement
  - Migration, asylum and border control management Administration of justice and democratic processes
- Not every AI system in these fields is high-risk
- List is updated regularly (12 months, Article 84)





# High-Risk AI Systems (Art. 6)

What governance infrastructure do you have in place for your AI systems?

High-risk AI systems must both conform to stringent quality standards and comply with disclosure, control, and monitoring requirements.

## Risk Management System

- Iterative and continuous process including suitable testing.
- Estimation, evaluation and preparation for known foreseeable risks and more.

## Record Keeping

- Designed with automatic record keeping of events ('logs'):
  - Period of each use of the system
  - Natural persons involved in the verification of the results

## Robustness, Accuracy and Cybersecurity

- Designed to achieve an appropriate level of accuracy, robustness and cybersecurity throughout the lifecycle
- Appropriate levels are declared in the documentation of the AI system

## Data and Data Governance

- Appropriate data governance & data management techniques must be applied
- High quality data sets & data governance:
  - Train validate test data sets
  - Relevant, representative, complete & free of errors
  - Prior assessment for availability, quantity, suitability, bias of the data

## Transparency & Information

- Provision of information to users
- System should be accompanied by instructions for use
- concise, complete, correct and clear information that is relevant, accessible and comprehensible to users:
  - Characteristics and limitations of the AI system

## Technical Documentation

- Continuous updating
- Before placement on market

## Human Oversight

- Human interface tools have to be integrated
- Possibility to find signs of anomalies, dysfunctions and unexpected performance
- Ability not to use the AI system to override, stop or reverse output



## Limited or Low-Risk AI Systems (Art. 6)

Are your users made aware they are interacting with an AI system?

While focused on high-risk, the regulation prescribes transparency and voluntary conduct for lower-risk applications.

### New transparency obligations for certain AI systems (Art. 52)

- Notify people that they are interacting with an AI system, unless this is obvious
- Notify people if emotional biometric or recognition categorization systems are applied
- Apply labels to deep fakes (with certain exceptions) or other manipulated content

### Possible voluntary code of conduct for AI with specific transparency requirements (Art. 69)

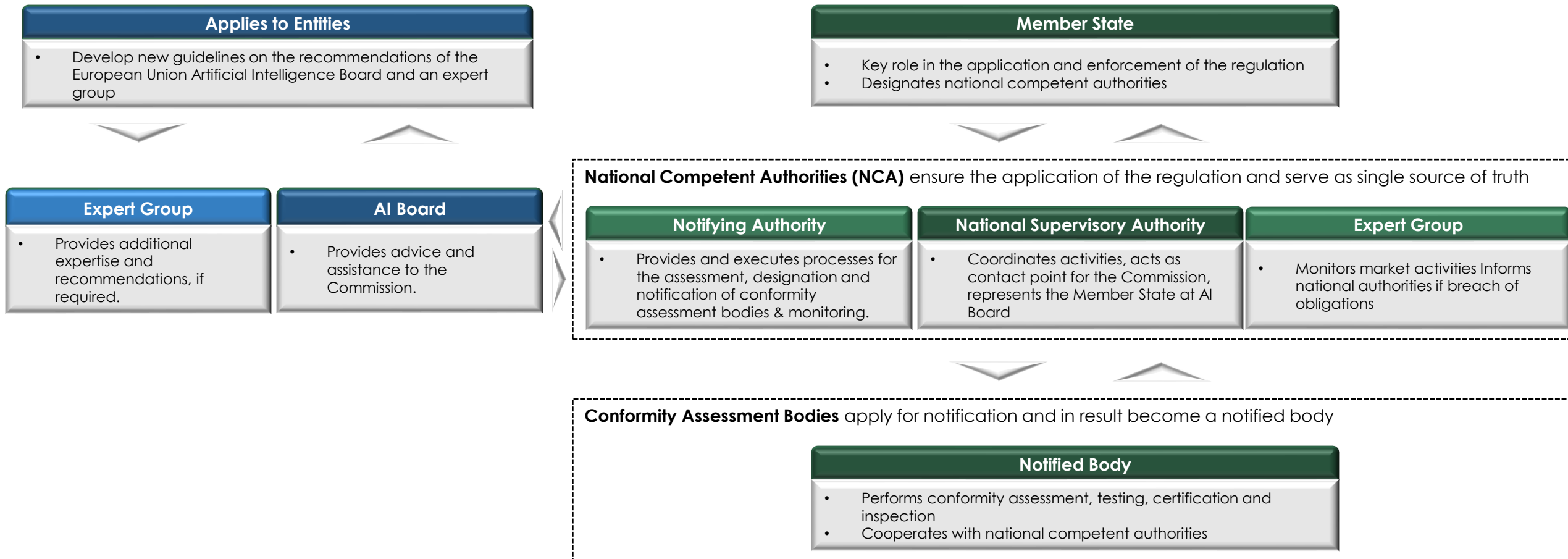
- No mandatory obligations
- Commission and Board will define codes of conduct intended to foster the voluntary application of requirements to low-risk AI systems
- Might include environmental sustainability or accessibility to persons with a disability
- Codes of Conduct can also be defined individually



# Governance Structure

With which regulators do you interact already now concerning AI?

The EU AI Act follows a clear chain of responsibility across national and supranational entities.

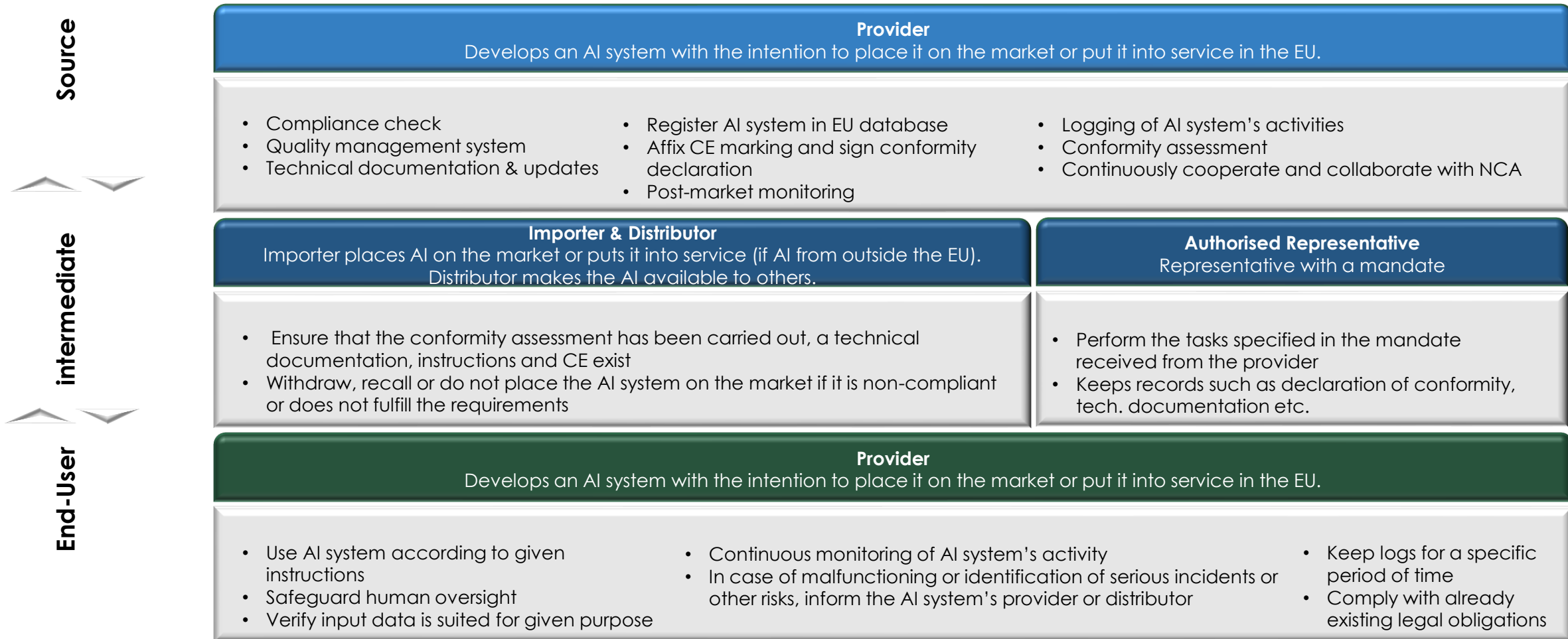




# Stakeholders, Roles and Obligations

Which roles are relevant to you?

Stakeholders are interconnected and each must fulfill specific obligations.

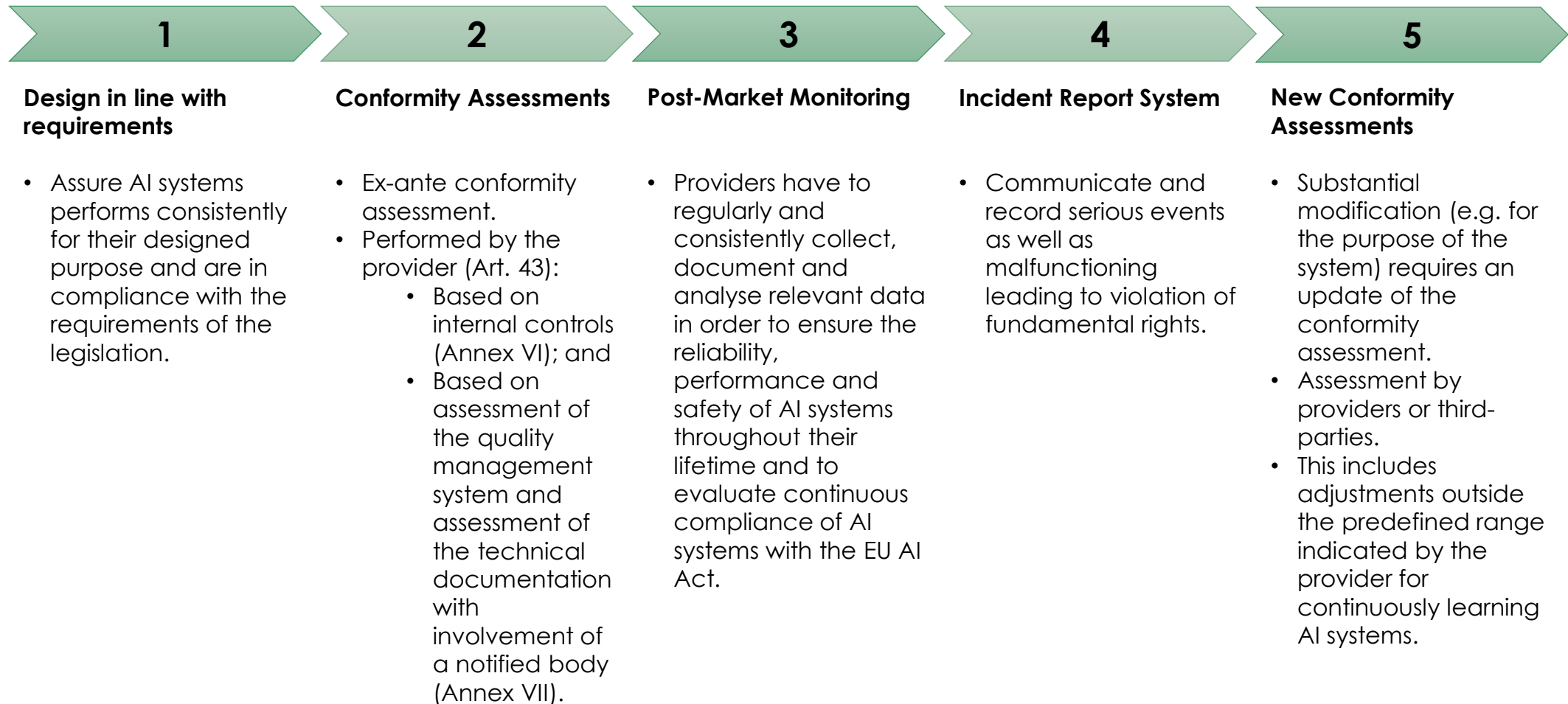




# Conformity Throughout the AI Lifecycle

Does your governance process include declarations of quality? Monitoring?

Product launch is only the beginning of compliance obligations for high-risk AI systems.





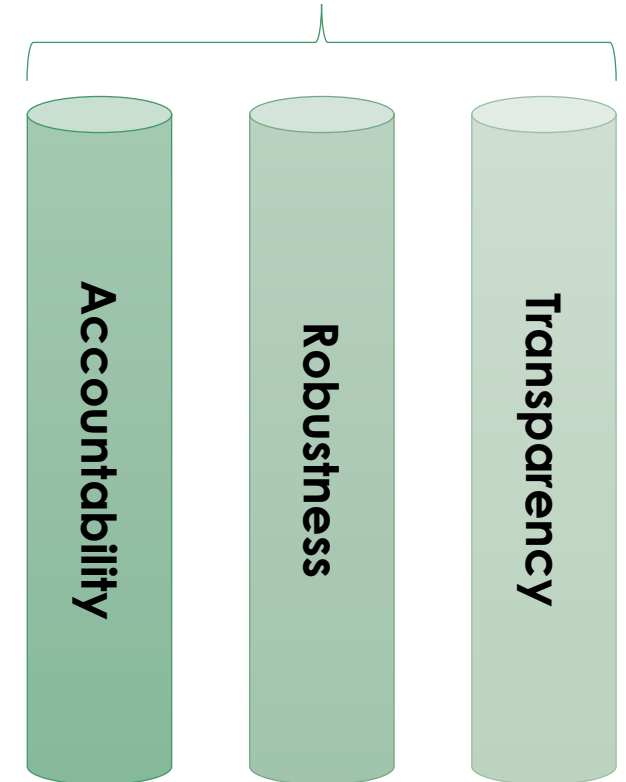
# We Are Ready, Are You?

Is there a gap between the AI Act and your standards? How large is it?

The proposed regulation lays forth requirements for AI within the EU. It will usher in change. We offer a path forward.

- The proposed regulation focuses on **ethical application** of AI, that use cases are **responsible**, that practitioners are **accountable** for upholding stringent quality standards.
- This includes general principles of **fair & impartial** treatment of subjects (regardless of the AI application), but also explicitly forbids certain applications.
- It specifically highlights high-risk applications and prescribes extensive disclosure accompanied by rigorous controls to ensure AI systems are **robust & reliable**.
- To ensure **safe & secure** operation of AI, the regulation demands human oversight, the ability to assume control or override the AI.
- Even for applications deemed lower risk, the Artificial Intelligence Act demands that AI systems are sufficiently **transparent**, alerting subjects to processing by AI, and that they are **explainable**, enabling their designers to monitor them effectively.
- The proposed regulation is grounded in the fundamental rights of the citizen, guarding against exploitation of vulnerabilities, ensuring due process, defending the rights of children, among others. It **preserves privacy** by outright forbidding applications of AI for the live, remote surveillance of citizens.

## AI & Partners' Pillars of Trustworthy AI Framework





# Your Path Towards Compliance

What has to change in your AI processes to integrate the AI Act?

The proposed regulation requires a declaration of conformity and CE marking prior to launch a high-risk AI system, as well as longer-term monitoring through end-of-life...

## 1. Identification

- Conduct a close examination of your existing assets and find out which ones use AI or qualify as AI under the new regulation.

## 3. Compliance

- Ensure design, development and quality management system are in compliance with the AI regulation.

## 5. Declaration

- Write a Declaration of conformity (Annex V) for each (high-risk) AI system and affix the CE marking.\*

## 7. Monitoring

- After launching the high-risk AI system, it needs to be monitored because the system learns

## 1. Identification

- Conduct a close examination of your existing assets and find out which ones use AI or qualify as AI under the new regulation.

## 4. Conformity Assessment

- High-risk AI systems must undergo a specified conformity assessment (Art. 19 and 43) and must repeat this step if they are substantially modified.

## 6. Market Launch

- Placing the high-risk AI system on the market or into service.

An **AI & Partners** tool designed to help businesses efficiently **govern and manage the risks associated with the use of Artificial Intelligence systems** throughout the lifecycle.

The workflow guides users through labyrinth of detailed questions to accurately assess risk. Straightforward and clear results are rendered on dashboards.

\*The CE marking indicates that an asset complies with the requirements stated in the AI regulation.



# Team



**Sean Musch**

Director

Risk Advisory | AI & Data Analytics

AI & Partners  
Amsterdam | Netherlands

[s.musch@ai-and-partners.com](mailto:s.musch@ai-and-partners.com)  
<https://www.ai-and-partners.com/>



**Michael Borrelli**

Director

Consulting | Artificial Intelligence

AI & Partners  
London | United Kingdom

[m.borrelli@ai-and-partners.com](mailto:m.borrelli@ai-and-partners.com)  
<https://www.ai-and-partners.com/>





# DISCLAIMER

This Presentation may contain information, text, data, graphics, photographs, videos, sound recordings, illustrations, artwork, names, logos, trade marks, service marks, and information about us, our lines of services, and general information may be provided in the form of documents, podcasts or via an RSS feed (“the Information”).

Except where it is otherwise expressly stated, the Information is not intended to, nor does it, constitute legal, accounting, business, financial, tax or other professional advice or services. The Information is provided on an information basis only and should not be relied upon. If you need advice or services on a specific matter, please contact us using the contact details for the relevant consultant or fee earner found on the Presentation.

The Presentation and Information is provided “AS IS” and on an “AS AVAILABLE” basis and we do not guarantee the accuracy, timeliness, completeness, performance or fitness for a particular purpose of the Presentation or any of the Information. We have tried to ensure that all Information provided on the Presentation is correct at the time of publication. No responsibility is accepted by or on behalf of us for any errors, omissions, or inaccurate information on the Presentation. Further, we do not warrant that the Presentation or any of the Information will be uninterrupted or error-free or that any defects will be corrected.

Although we attempt to ensure that the Information contained in this Presentation is accurate and up-to-date, we accept no liability for the results of any action taken on the basis of the Information it contains and all implied warranties, including, but not limited to, the implied warranties of satisfactory quality, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy are excluded from these Terms to the extent that they may be excluded as a matter of law.

In no event will we be liable for any loss, including, without limitation, indirect or consequential loss, or any damages arising from loss of use, data or profits, whether in contract, tort or otherwise, arising out of, or in connection with the use of this Presentation or any of the Information.



AI  
AI & Partners

**QUESTIONS?**



AI  
AI & Partners

**THANK YOU FOR YOUR TIME**

**AI & Partners**

**Sean Musch**

s.musch@ai-and-partners.com

+31 (6) 57285579

**Michael Charles Borrelli**

m.borrelli@ai-and-partners.com

+44(0)7535 994 132



<https://www.ai-and-partners.com/>