

Artificial Intelligence Act

2023

Risk Advisory – Deloitte Czech Republic

The *Artificial Intelligence Act* in a Nutshell

The Proposal for a regulation is laying down harmonized rules on artificial intelligence.

Where do you see the AI Act impacting you?



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?

- According to a member of the European commission the implementation and ratification process could take 2-3 years



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
- Deloitte with Trustworthy AI has the necessary competence



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

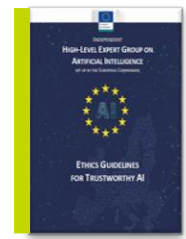
A Proposal 2 Years in the Making

In total, 1215 institutions or individuals contributed to this proposal, the overall agreement is a need for action.

How does the AI Act surprise vs prior papers?

- DATA
- GDPR
- Artificial Intelligence

EU focus on leading international regulation and driving innovation



EC Guidelines
Ethics guidelines for trustworthy AI
8th April 2019



EC Paper
A European strategy for data
19th February 2020



AEPD Guide
GDPR Adaptation to AI products and services
13th February 2020



EC Report
Safety and liability implications of Artificial Intelligence, the Internet of Things and robotics
19th February 2020



EC Paper
White paper on artificial intelligence
19th February 2020



EP Study
The impact of the General Data Protection Regulation (GDPR) on artificial intelligence
15th July 2020



EC Assessment List
Trustworthy Artificial Intelligence (ATAI) for self-assessment
17th July 2020



EP Study
Artificial Intelligence and Law Enforcement
13th July 2020



EP Study
Artificial Intelligence and Civil Liability (Legal Affairs)
13th July 2020



EC Proposal paper
Data Governance Act
25th November 2020



EP Study
Civil liability regime for artificial intelligence
18th September 2020



EP Study
EU framework on ethical aspects of artificial intelligence, robotics and related technologies
20th September 2020



Regulation on a European Approach for Artificial Intelligence
21st April 2021

Regulation on a European Approach for Artificial Intelligence enters into force



The Goal of the AI Act

The proposal lays out a legislative framework for dealing with AI in the future - with the goal of driving innovation and mitigating risks.

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

AI Act is about...



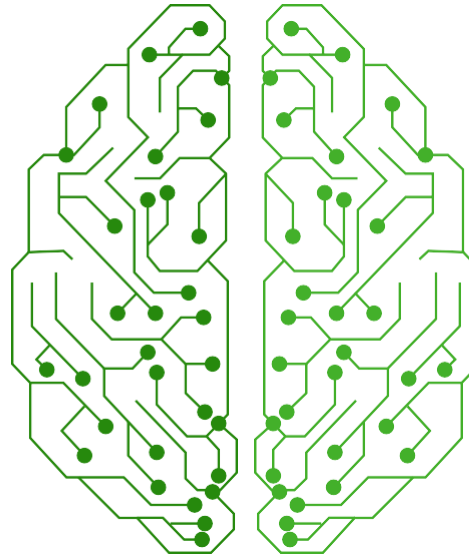
Emphasizing the **ethical application of AI**, instilling European values while improving transparency.



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.



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**.



Ensuring **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.



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 or obligations may result in a fine of **€20M or 4% of global annual turnover**.

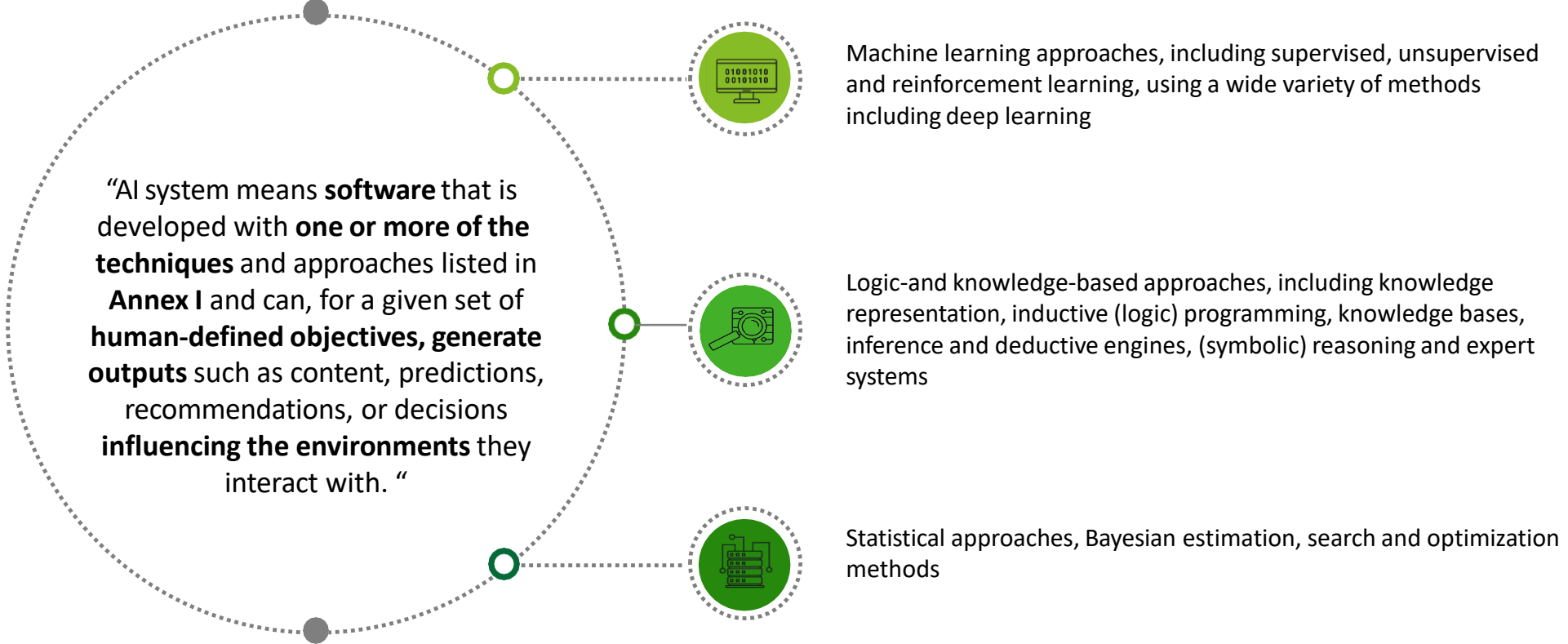


Incorrect, misleading information submitted to notified bodies or NCAs: **€10M or 2% global annual turnover**.

A Broad Definition of AI

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

What models do you have that the AI Act would consider as AI?



Comprehensive

cover all current and future AI including machine learning, deep learning as well as hybrid systems



Future proof

by focusing more on the use cases than on AI technology itself + complementary to existing legislation, especially GDPR



Legally secure

neutral as possible in regards to technical details in order to cover techniques which are not yet known or developed

The Scope of the Artificial Intelligence Act

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

*How are you affected? As a provider?
An importer? A distributor? A User?*

Requirements and Obligations of the 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

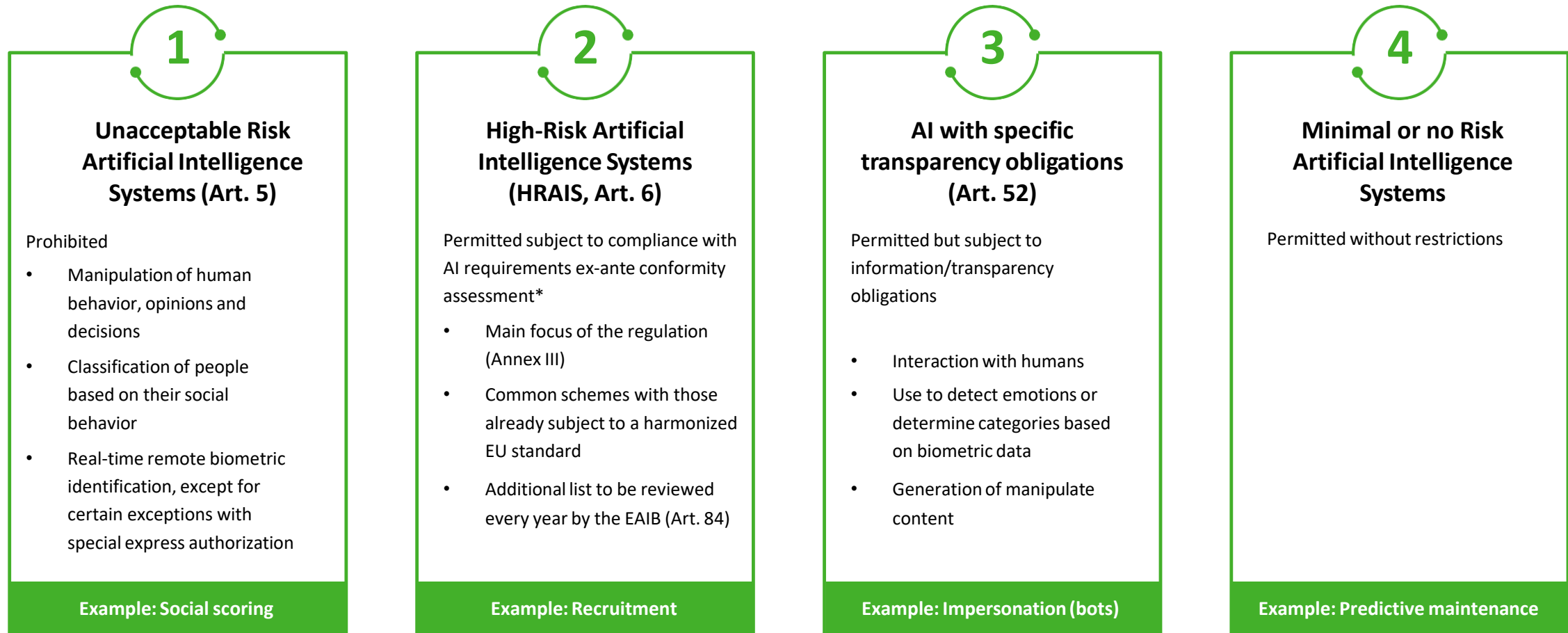
Entities Out of Scope

- 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

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

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



*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 Artificial Intelligence Systems (Art. 5)

Applications of AI that pose an unacceptable risk are prohibited.

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

1

Subliminal manipulation resulting in physical/psychological harm

Example: To push truck drivers to drive longer than healthy and safe, an inaudible sound 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 behavior 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 “misbehavior”.

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.

High-Risk Artificial Intelligence Systems (HRAIS, Art. 6)

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

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

High-risk AI systems (Article 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:
 1. Biometric identification and categorization of natural persons
 2. Management and operation of critical infrastructure
 3. Education and vocational training
 4. Employment, workers management and access to self-employment
 5. Access to and enjoyment of essential private services and public services and benefits
 6. Law enforcement
 7. Migration, asylum and border control management
 8. 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 Artificial Intelligence Systems (HRAIS, Art. 6)

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

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

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

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

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

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

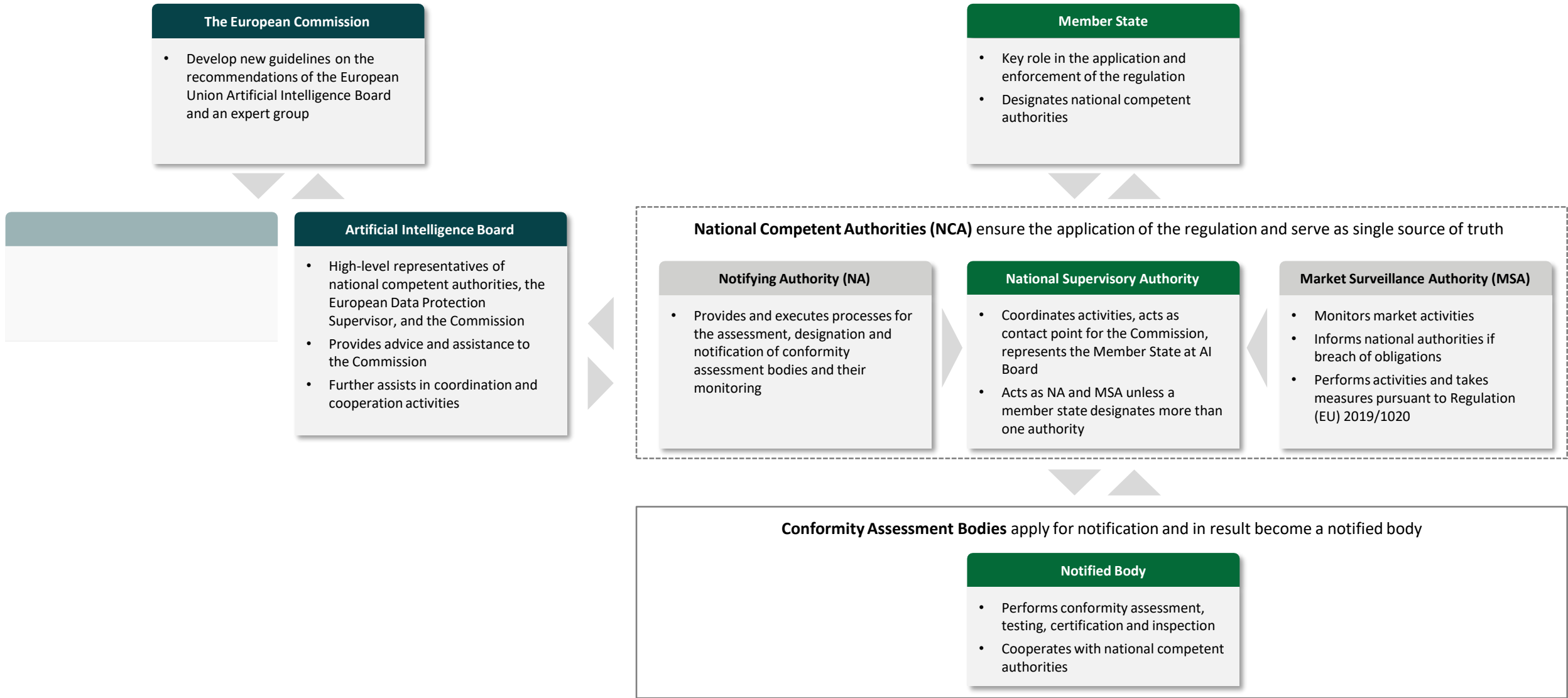
Possible voluntary code of conduct for AI with specific transparency requirements (Art. 69)

- 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

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

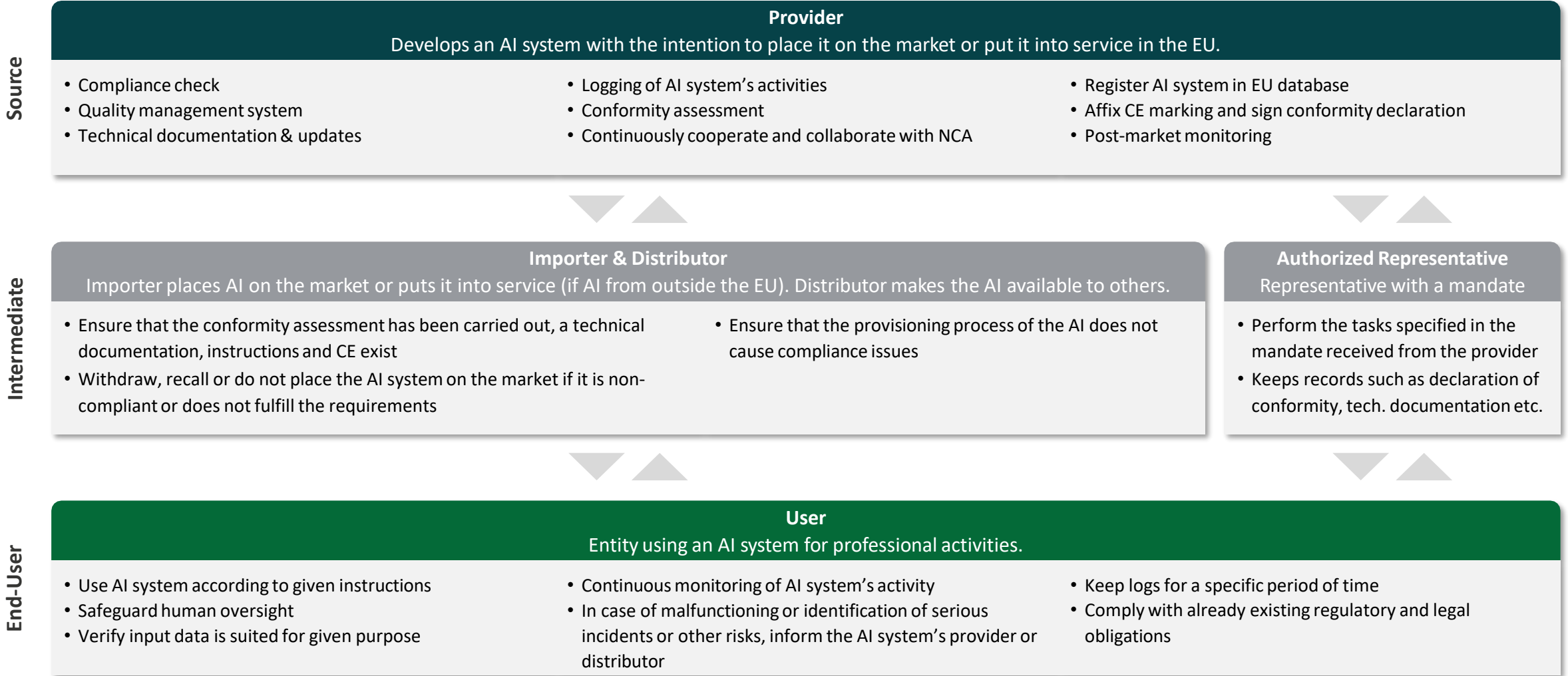
With which regulators do you interact already now concerning AI?



Stakeholders, Roles and Obligations

Stakeholders are interconnected and each must fulfill specific obligations.

Which roles are relevant to you?



Conformity Throughout the AI Lifecycle

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

Does your governance process include declarations of quality? Monitoring?

1. Design in line with requirements

- Assure AI systems performs consistently for their designed purpose and are in compliance with the requirements of the Regulation



2. Conformity assessment

- Ex-ante Conformity assessment
- Performed by the provider (Art. 43):
 - Based on internal controls (Annex VI)
 - Based on assessment of the quality management system and assessment of the technical documentation with involvement of a notified body (Annex VII)

5. New Conformity assessment

- Substantial modification (e.g., purpose of the system) requires an update of the conformity assessment
- Assessment by providers or any third-party
- This includes adjustments outside the predefined range indicated by the provider for continuously learning AI systems

3. Post-market monitoring

- Providers have to regularly and consistently collect, document and analyze relevant data in order to ensure the reliability, performance and safety of AI systems throughout their lifetime and to evaluate continuous compliance of AI systems with the Regulation

4. Incident report system

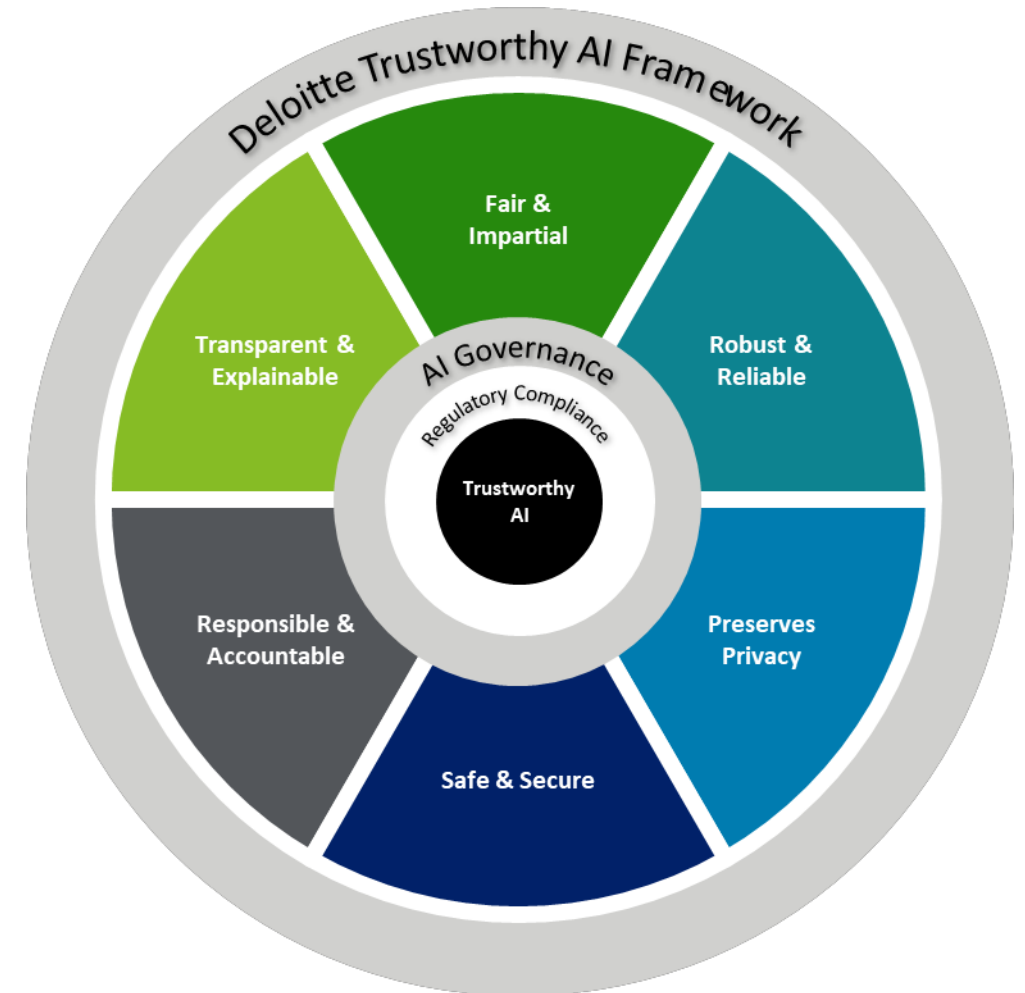
- Communicate and record serious events as well as malfunctioning leading to violation of fundamental rights

We Are Ready, Are You?

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

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

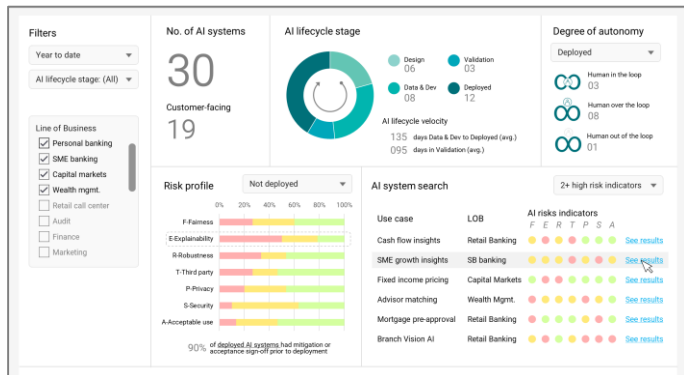
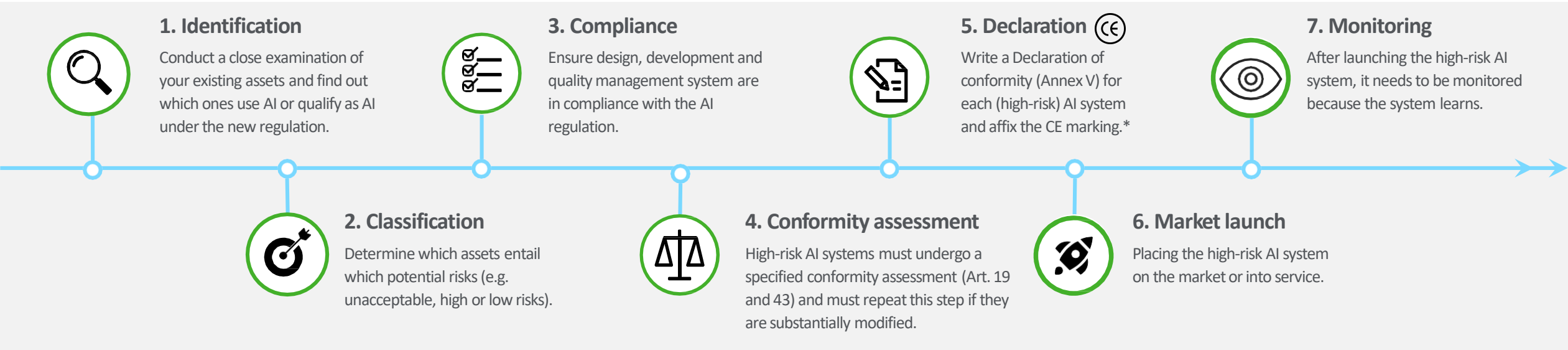
- The proposed regulation focuses on **ethical application** of AI, that use cases are **responsible**, that practitioners are **accountable** for upholding stringent quality standards.
- This includes general principles of **fair & impartial** treatment of subjects (regardless of the AI application), 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.



Your Steps Towards Compliance

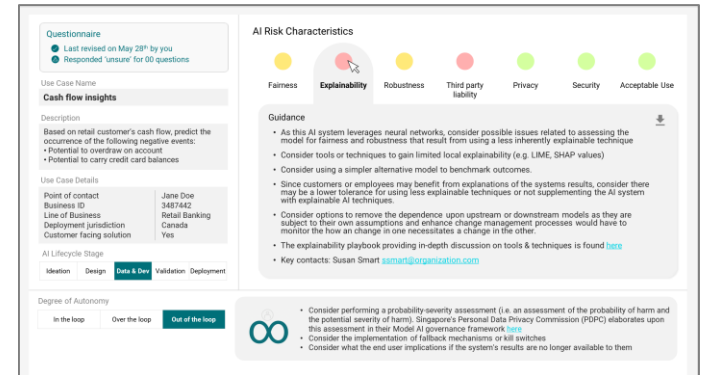
The proposed regulation requires a declaration of conformity and CE marking prior to launch a high-risk AI system, as well as longer-term monitoring through end-of-life...

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



A Deloitte tool designed to help organizations 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.



Contacts

Trustworthy AI



Jakub Höll

Director
Risk Advisory

Kontakt:

jholl@deloittece.com

+420 734 353 815



Vilém Krejcar

Consultant
Risk Advisory

Contact:

vkrejcar@deloittece.com

+420 778 438 998



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/cz/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, legal, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, the member firm in Central Europe of Deloitte Touche Tohmatsu Limited. Services are provided by the subsidiaries and affiliates of Deloitte Central Europe Holdings Limited, which are separate and independent legal entities. The subsidiaries and affiliates of Deloitte Central Europe Holdings Limited are among the region's leading professional services firms, providing services through more than 6,000 people in 44 offices in 18 countries.

© 2023. For more information, contact Deloitte Czech Republic.