Responsible AI

PvIB – Utrecht

—

13 februari 2024

Agenda

01 Introduction

02 EU Digital Single Market

03 AI Act

04 Wrap-up

With you today

Erik van den Berg

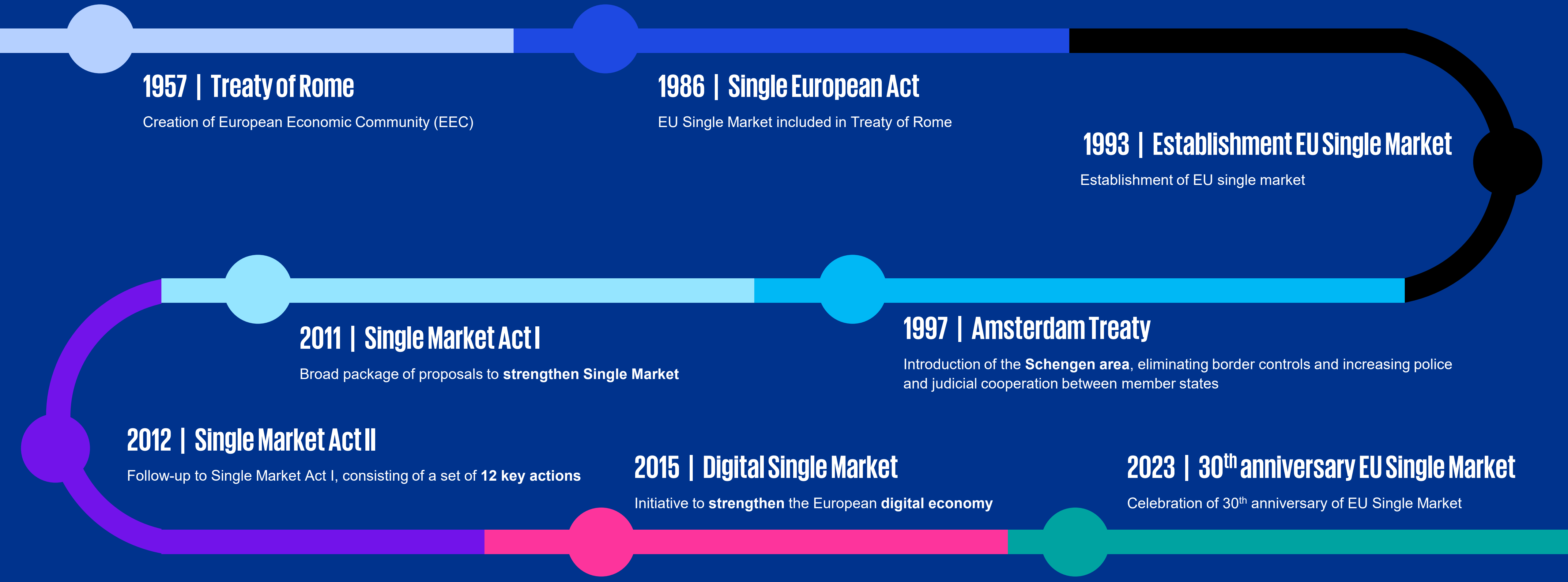
Consultant Digital Law
Vandenberg.erik@kpmg.nl
+31 6 5791 5720

Jasper Oomen

Consultant Digital Law
Oomen.jasper@kpmg.nl
+31 6 1898 3712

EU (Digital) Single Market

History of the EU Single Market



1957 | Treaty of Rome

Creation of European Economic Community (EEC)

1986 | Single European Act

EU Single Market included in Treaty of Rome

1993 | Establishment EU Single Market

Establishment of EU single market

1997 | Amsterdam Treaty

Introduction of the **Schengen area**, eliminating border controls and increasing police and judicial cooperation between member states

2011 | Single Market Act I

Broad package of proposals to **strengthen Single Market**

2012 | Single Market Act II

Follow-up to Single Market Act I, consisting of a set of **12 key actions**

2015 | Digital Single Market

Initiative to **strengthen** the European **digital economy**

2023 | 30th anniversary EU Single Market

Celebration of 30th anniversary of EU Single Market

1993 | Establishment EU Single Market

Establishment of EU single market

European Single Market | the four freedoms

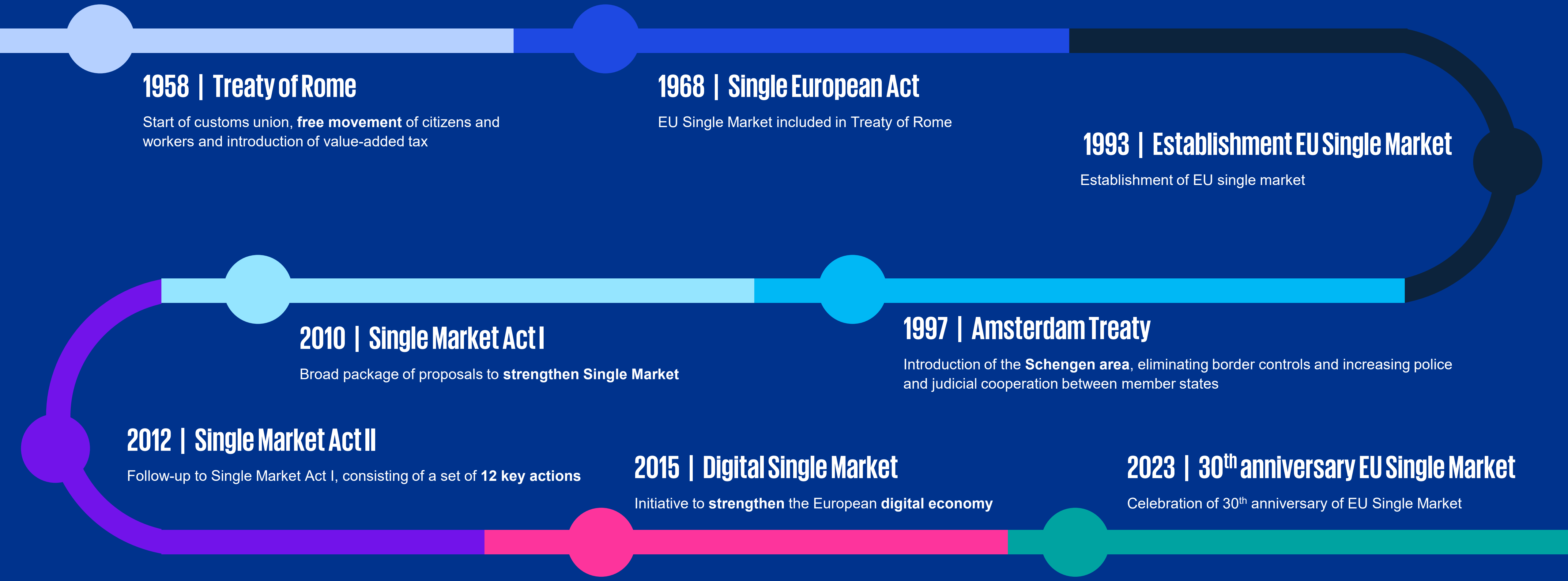
Free movement of goods

Free movement of persons

Free movement of services

Free movement of capital

History of the EU Single Market



1958 | Treaty of Rome

Start of customs union, **free movement** of citizens and workers and introduction of value-added tax

1968 | Single European Act

EU Single Market included in Treaty of Rome

1993 | Establishment EU Single Market

Establishment of EU single market

1997 | Amsterdam Treaty

Introduction of the **Schengen area**, eliminating border controls and increasing police and judicial cooperation between member states

2010 | Single Market Act I

Broad package of proposals to **strengthen Single Market**

2012 | Single Market Act II

Follow-up to Single Market Act I, consisting of a set of **12 key actions**

2015 | Digital Single Market

Initiative to **strengthen** the European **digital economy**

2023 | 30th anniversary EU Single Market

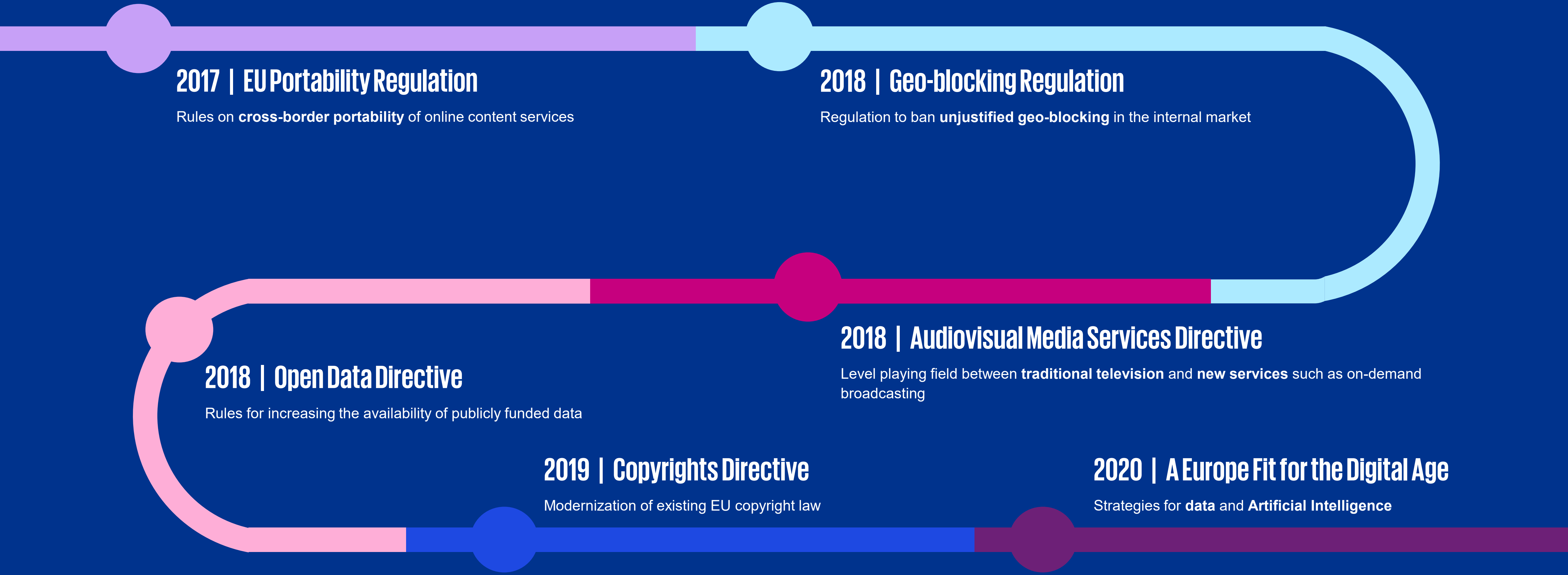
Celebration of 30th anniversary of EU Single Market

Introduction of the EU Digital Single Market

2015 | Digital Single Market

Initiative to **strengthen** the European **digital economy**

Establishment EU Digital Single Market



2017 | EU Portability Regulation

Rules on **cross-border portability** of online content services

2018 | Geo-blocking Regulation

Regulation to ban **unjustified geo-blocking** in the internal market

2018 | Audiovisual Media Services Directive

Level playing field between **traditional television** and **new services** such as on-demand broadcasting

2018 | Open Data Directive

Rules for increasing the availability of publicly funded data

2019 | Copyrights Directive

Modernization of existing EU copyright law

2020 | A Europe Fit for the Digital Age

Strategies for **data** and **Artificial Intelligence**

Introduction of EU's Digital Strategy: A Europe Fit for the Digital Age

Three pillars of EU's Digital Strategy: A Europe Fit for the Digital Age

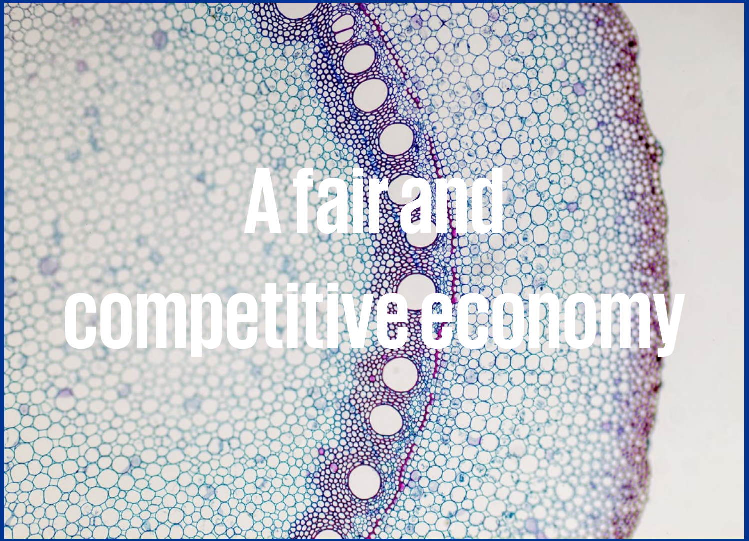
Technology that works for people

Key actions

A Digital Education Action Plan

European AI Strategy

A European Cybersecurity Strategy



A fair and competitive economy

Key actions

European Data Strategy

Industrial Strategy Package

New Consumer Agenda

An open, democratic and sustainable society

Key actions

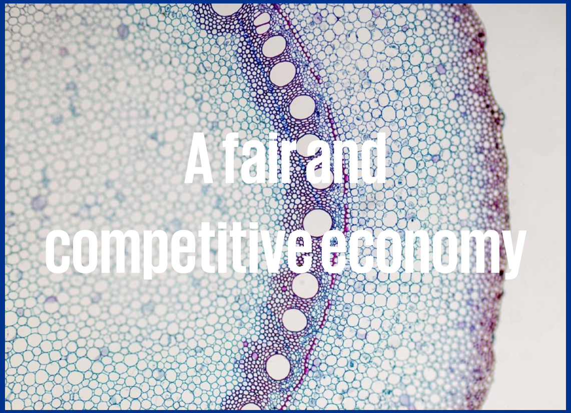
Circular Electronics Initiative

European Democracy Action Plan

Rules for Digital Services

Key EU Strategic Initiatives related to AI, Cybersecurity and Data

Technology that works for people



A fair and competitive economy

European AI Strategy

European Data Strategy

A European Cybersecurity Strategy

European Data Stategy

1

Data Governance Act

Framework for data sharing of (protected) public sector data, Data intermediation, and Data altruism

2

Data Act

Access and use of data generated by smart products, and government access to private data

A European Cybersecurity Strategy

1

NIS2

Cybersecurity requirements for essential entities

2

Cyber Resilience Act

Cybersecurity requirements for hardware and software products with digital elements

3

Cyber Solidarity Act

Cross-border Security Operations Centres, and ‘coordinated preparedness testing

European AI Strategy: A European approach to trust in AI

1

AI Act

Risk Based approach to ensure safe, transparant, ethical, unbiased and human controlled use of AI systems

2

AI Liability Directive

Non-contractual civil liability rules for damages caused by AI

3

General Product Liablity Directive (revision)

Rules on liability for software and AI

KPMG

European AI Strategy: A European approach to trust in AI

Ex ante

1

AI Act

Risk Based approach to ensure safe, transparant, ethical, unbiased and human controlled use of AI systems

Ex post

2

AI Liability Directive

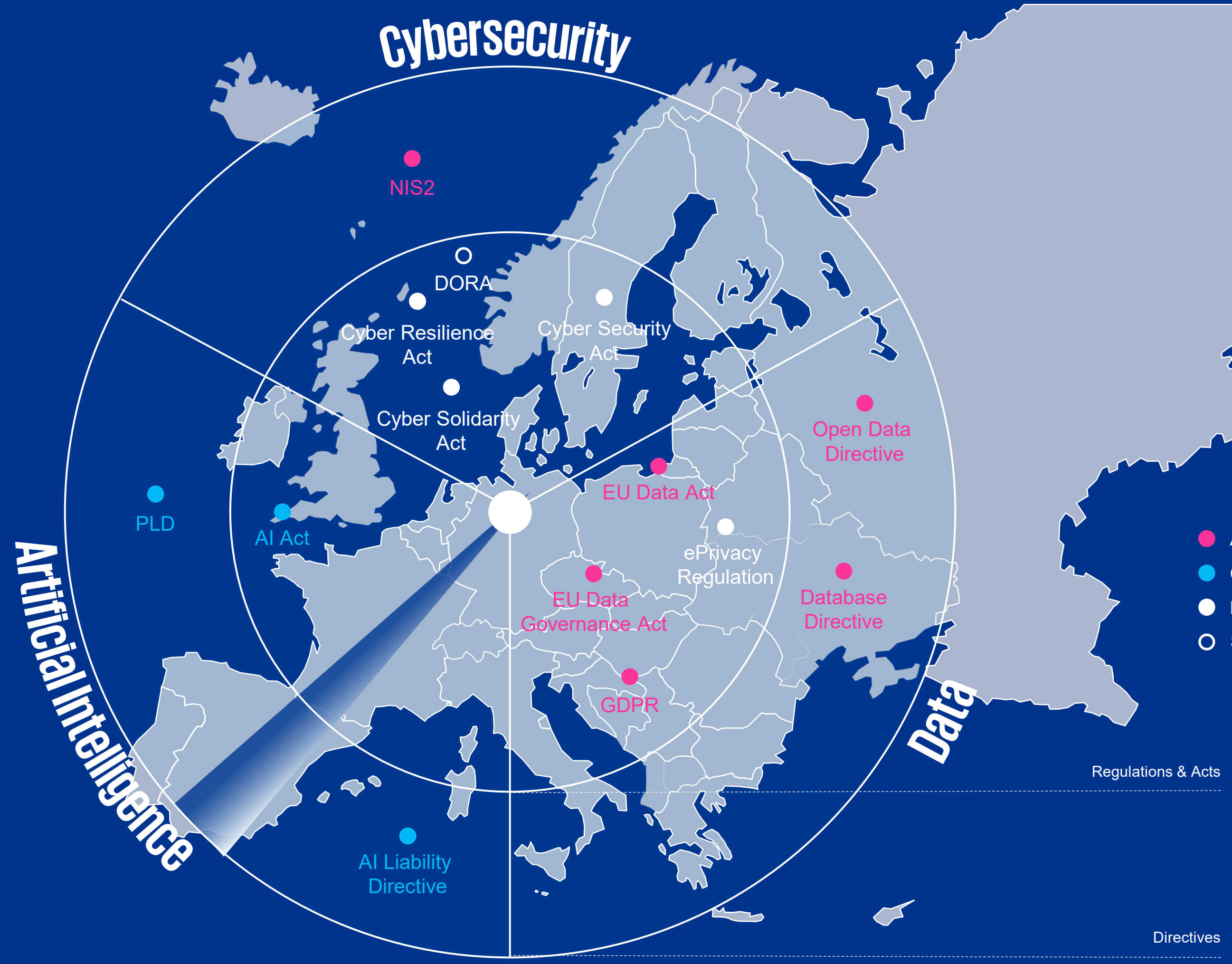
Non-contractual civil liability rules for damages caused by AI

3

General Product Liablity Directive (revision)

Rules on liability for software and AI

Legislative Initiatives from Key EU Strategic Initiatives



● Adopted

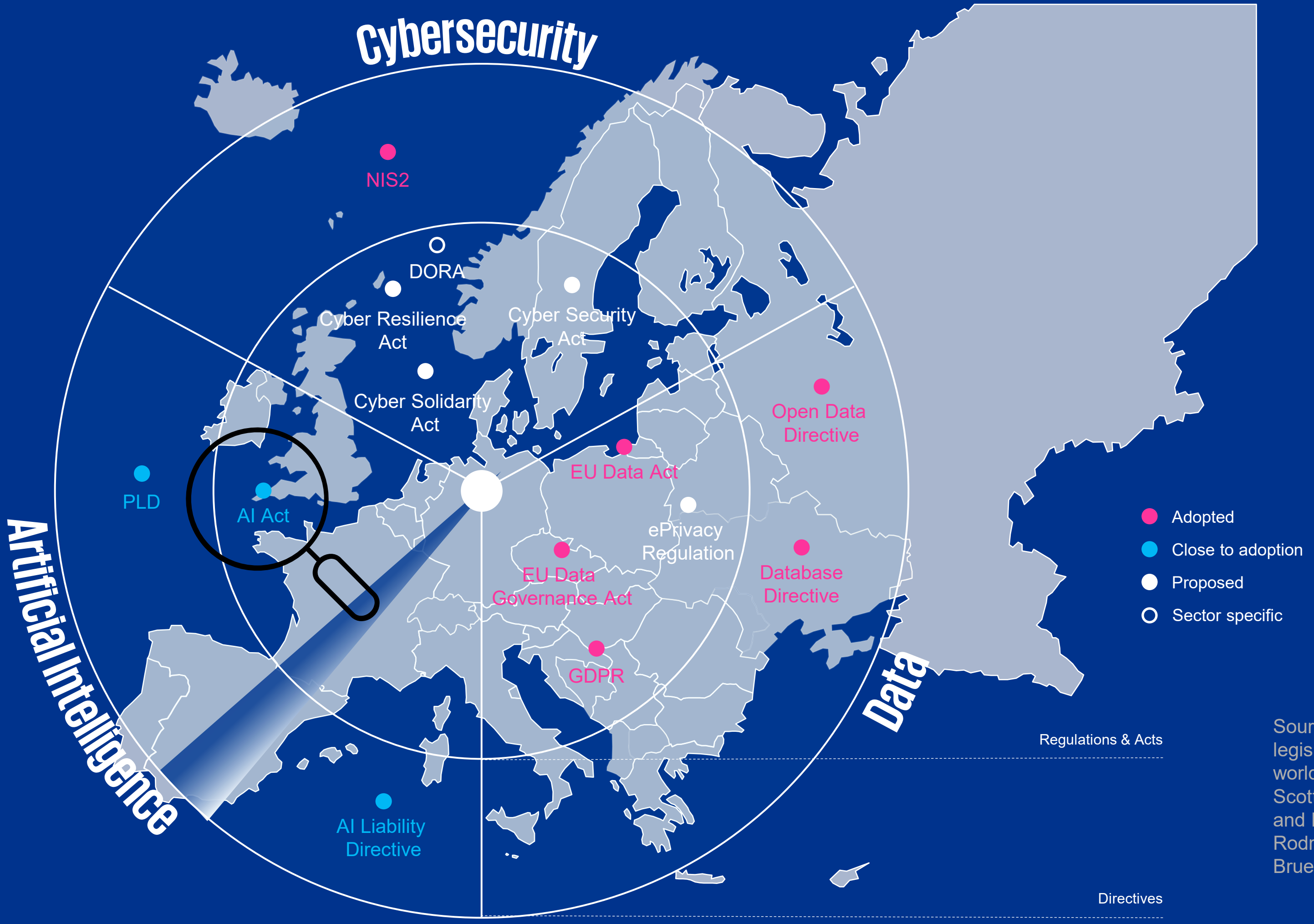
● Close to adoption

● Proposed

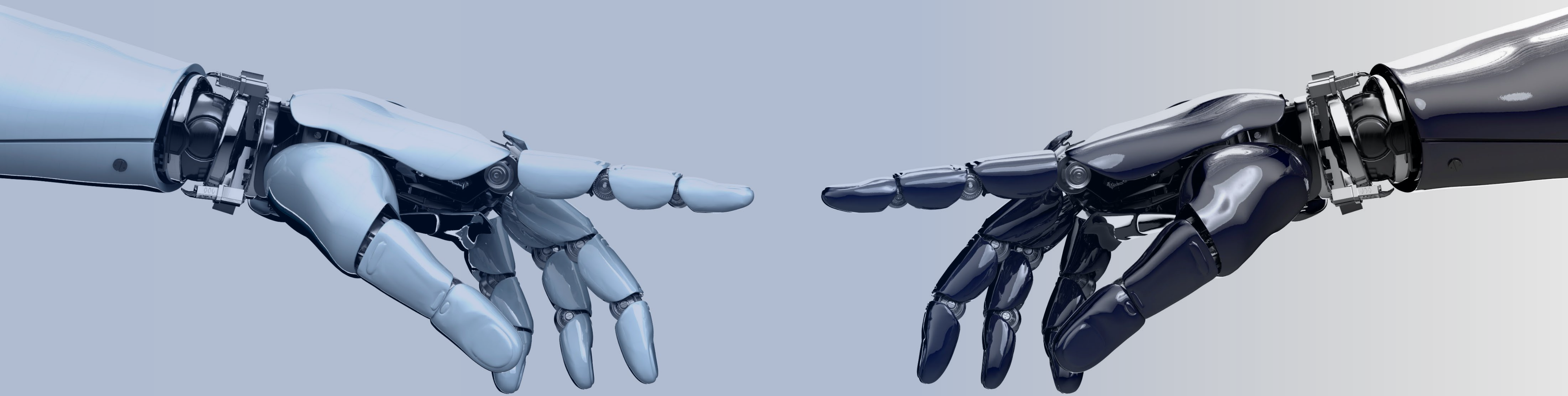
○ Sector specific

Source: 'A dataset on EU legislation for the digital world', Kai Zenner, J. Scott Marcus, Kamil Sekut and Hèctor Badenes Rodríguez published by Bruegel.

Legislative Initiatives from Key EU Strategic Initiatives

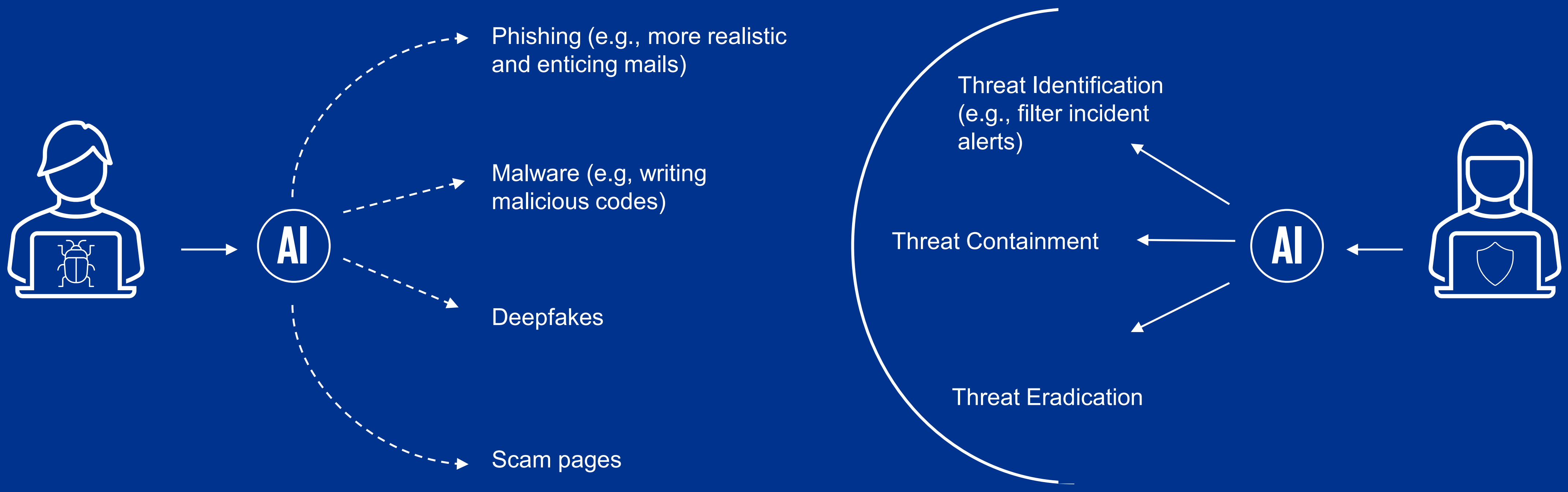


Source: 'A dataset on EU legislation for the digital world', Kai Zenner, J. Scott Marcus, Kamil Sekut and Hèctor Badenes Rodríguez published by Bruegel.



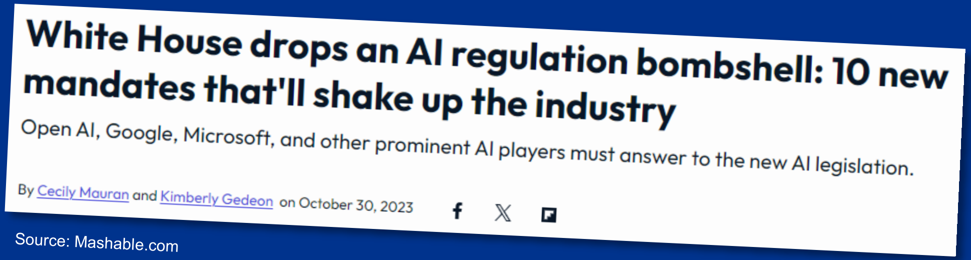
Artificial intelligence & AI Act

AI strengthens both Defenses and Threats of Cybersecurity



AI
Phishing (e.g., more realistic and enticing mails)
Malware (e.g, writing malicious codes)
Deepfakes
Scam pages
Threat Identification (e.g., filter incident alerts)
Threat Containment
Threat Eradication
AI

AI is at the top of the global political agenda

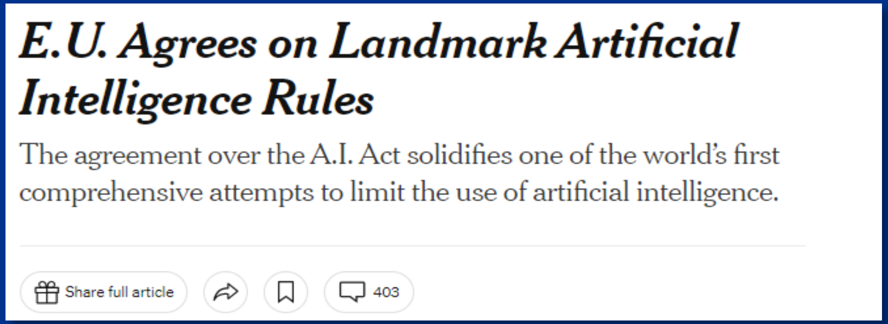


White House drops an AI regulation bombshell: 10 new mandates that'll shake up the industry

Open AI, Google, Microsoft, and other prominent AI players must answer to the new AI legislation.

By Cecily Mauran and Kimberly Gedeon on October 30, 2023

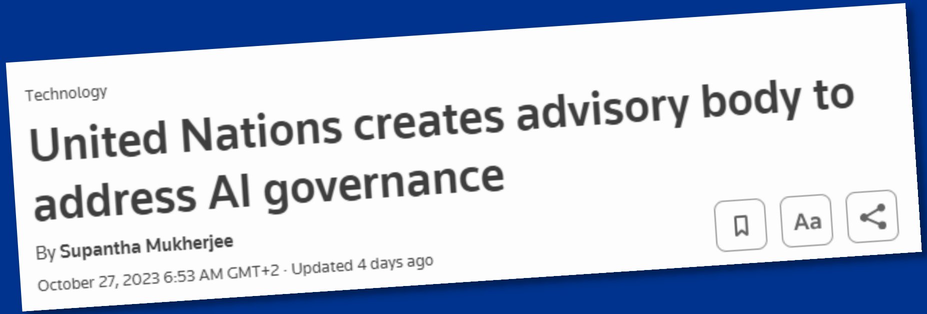
Source: Mashable.com



E.U. Agrees on Landmark Artificial Intelligence Rules

The agreement over the A.I. Act solidifies one of the world's first comprehensive attempts to limit the use of artificial intelligence.

Source: the New York Times



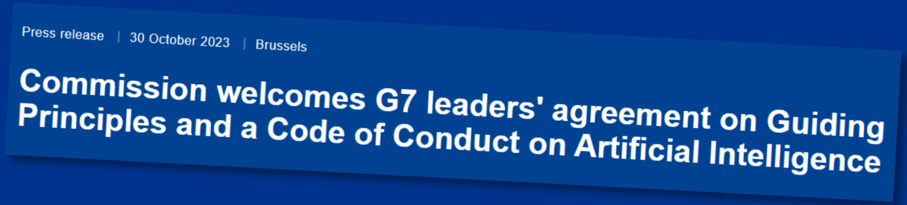
Technology

United Nations creates advisory body to address AI governance

By Supantha Mukherjee

October 27, 2023 6:53 AM GMT+2 · Updated 4 days ago

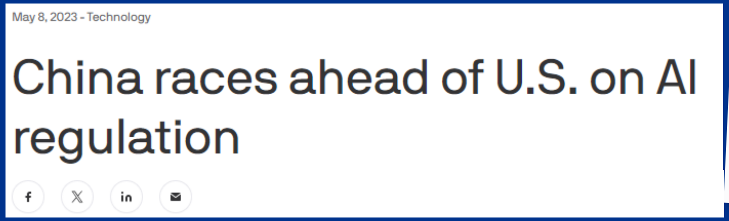
Source: Reuters.com



Press release | 30 October 2023 | Brussels

Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence

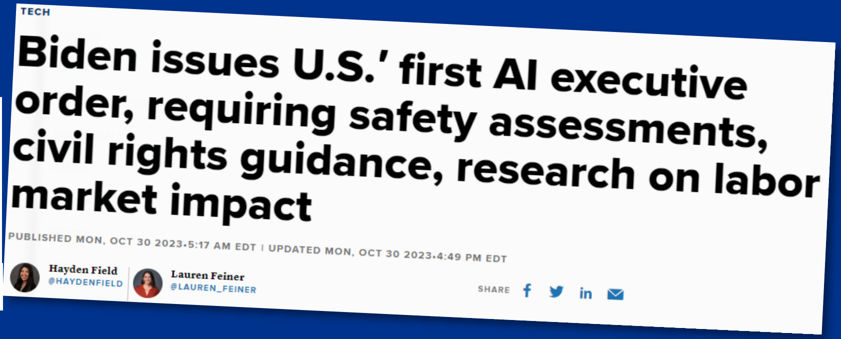
Source: European Commission



May 8, 2023 - Technology

China races ahead of U.S. on AI regulation

Source: Axios



TECH

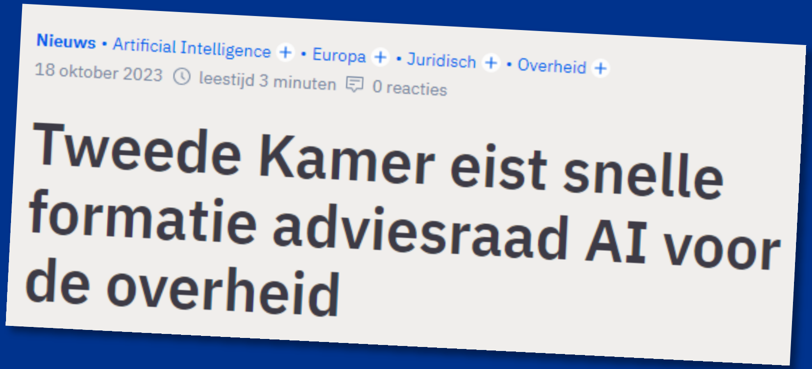
Biden issues U.S.' first AI executive order, requiring safety assessments, civil rights guidance, research on labor market impact

PUBLISHED MON, OCT 30 2023•5:17 AM EDT | UPDATED MON, OCT 30 2023•4:49 PM EDT

Hayden Field @HAYDENFIELD

Lauren Feiner @LAUREN_FEINER

Source: CNBC



Nieuws • Artificial Intelligence + • Europa + • Juridisch + • Overheid +

18 oktober 2023 leestijd 3 minuten 0 reacties

Tweede Kamer eist snelle formatie adviesraad AI voor de overheid

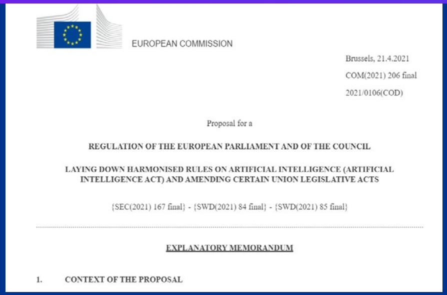
Source: Agconnect.com

The AI Act is expected to enter into force mid-2024

2019

Announcement of 'A Europe fit for the digital age'

2021



EUROPEAN COMMISSION

Brussels, 21.4.2021
COM(2021) 206 final
2021/0106(COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

European Commission proposes AI Act

Start-2024

Approval final draft text AI Act

Mid-2024

Expected adoption AI Act

Start-2025

First obligations expected to apply

The AI Act in a nutshell

Stimulate the good

- Stimulate innovation through **regulatory sandboxes**
- Stimulate **harmonization** of standards, codes of conduct and certification
- Offer greater **transparency** regarding AI systems
- Create **level playing field** for actors involved
- **Safeguard fundamental rights** and provide legal certainty for EU citizens

Fix the bad

- Impose **stricter requirements** for high-risk AI systems (obligatory risk management, data governance, technical documentation, etc.)
- Carry out **conformity assessments** and post-market monitoring for high-risk AI systems
- **Avoid fundamental rights violations**
- Establish **effective oversight** and enforcement mechanisms

Control the ugly

- **Prohibit unacceptable-risk** AI systems
- **Prevent use of subliminal techniques** that distort a person's behavior in such a way that it causes harm to that person or another person
- **Prohibit exploitation of vulnerabilities** of a specific group of persons, e.g. exploiting age or disability.

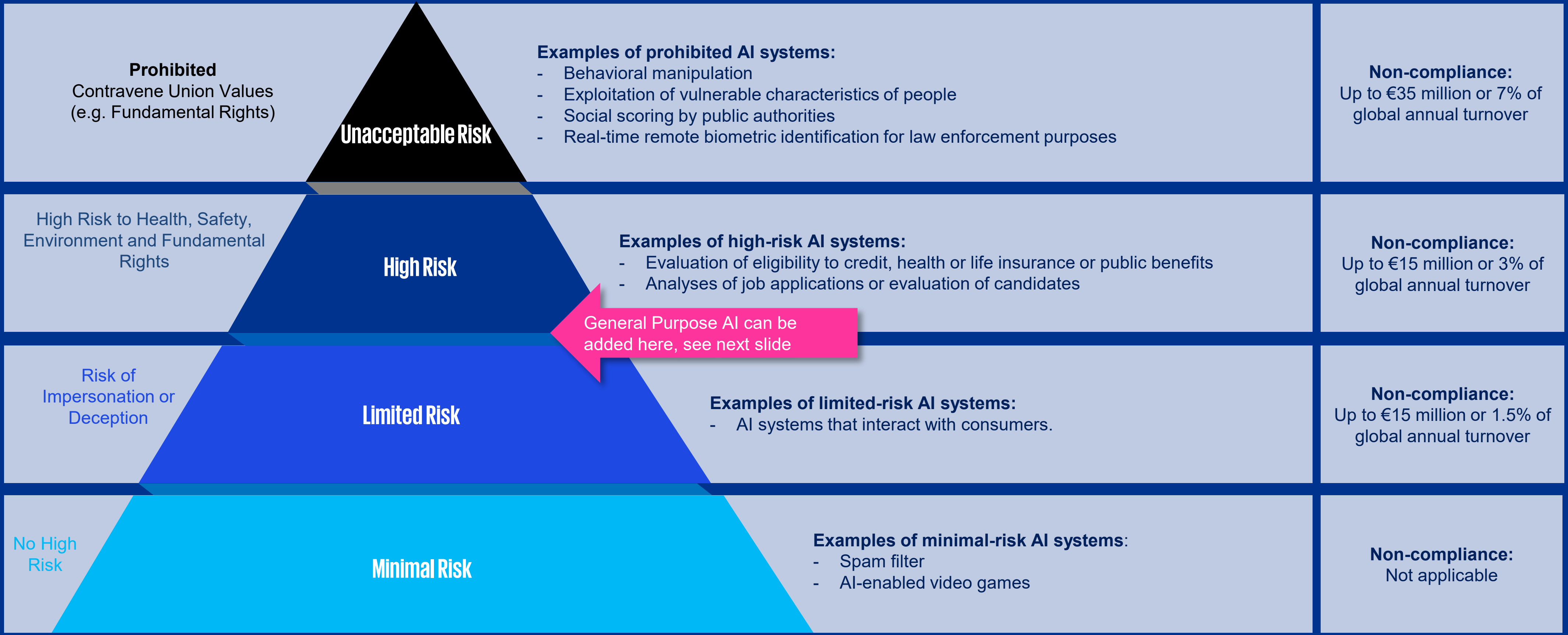
The AI Act will apply to all AI systems built or deployed in EU markets.

What is an AI system under the AI Act?

“

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’

The AI Act follows a risk-based approach



Prohibited Contravene Union Values (e.g. Fundamental Rights)	Unacceptable Risk	**Examples of prohibited AI systems:** - Behavioral manipulation - Exploitation of vulnerable characteristics of people - Social scoring by public authorities - Real-time remote biometric identification for law enforcement purposes	**Non-compliance:** Up to €35 million or 7% of global annual turnover
High Risk to Health, Safety, Environment and Fundamental Rights	High Risk	**Examples of high-risk AI systems:** - Evaluation of eligibility to credit, health or life insurance or public benefits - Analyses of job applications or evaluation of candidates	**Non-compliance:** Up to €15 million or 3% of global annual turnover
Risk of Impersonation or Deception	Limited Risk	**Examples of limited-risk AI systems:** - AI systems that interact with consumers.	**Non-compliance:** Up to €15 million or 1.5% of global annual turnover
No High Risk	Minimal Risk	**Examples of minimal-risk AI systems**: - Spam filter - AI-enabled video games	**Non-compliance:** Not applicable

General Purpose AI can be added here, see next slide

Notable exceptions:

The latest version of the AI Act adds another category: General Purpose AI-system

> “
>
> ‘general purpose AI model’ means an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications. This does not cover AI models that are used before release on the market for research, development and prototyping activities.

General Purpose AI model

Models like GPT, Gemini and Bard qualify as GPAI

This category sees specifically the models used, not the systems.

Providers of GPAI need to be transparent on the training data that was used.

Systemic Risk GPAI

Some General Purpose AI models are deemed to possess systemic risk when they operate with 10^25 Floating Point Operations.

Currently only GPT4.0 and maybe Gemini are expected to reach this threshold.

Additional requirements apply with regard to red teaming, cybersecurity, incident reporting and risk mitigation.

High Risk AI Systems

(Safety components of) AI systems qualifying as:

- In vitro diagnostic medical devices
- Machinery
- Lifts
- Appliances burning gaseous fuels
- Agricultural and forestry vehicles
- Marine equipment
- Motor vehicles and their trailers
- Medical devices
- Two- or three-wheel vehicles
- Personal protective equipment
- Radio equipment
- Toys
- Recreational craft and personal watercraft
- Civil aviation
- Rail system
- Pressure equipment

AI systems intended to be used for:

- Educational and vocational training
- Critical infrastructures
- Law enforcement
- Essential private and public services
- Administration of justice and democratic processes
- Migration, asylum and border control management
- Employment, workers management and access to self-employment
- Biometric identification of natural persons

Obligations in relation to High Risk AI systems

	Provider	*Distributor*	*Importer*	*Deployer*
Risk-management system	✓			
Data Governance and Management	✓			
Technical documentation	✓			
Record keeping	✓			
Transparency and provision of information to users	✓			
Human oversight	✓			✓
Accuracy, robustness and cybersecurity	✓			
Indication contact details	✓		✓	
Quality management system	✓			
Documentation keeping	✓			
Log keeping	✓			✓
Conformity assessment, EU declaration of conformity and affixion CE Marking	✓			
Verification of conformity assessment, technical documentation, CE Marking		✓	✓	
Corrective actions to achieve conformity		✓		
Provision of relevant information to and cooperation with national competent authority	✓	✓	✓	✓
(Monitor) use in accordance with instructions				✓
Use of Relevant input data				✓
Fundamental rights impact assessment				✓

Provider

Develop
Make significant changes
Change main purpose
Place on market under own name

Deployer

Use under own authority other than in the course of a personal non-professional activity

Importer

Place on the market from legal person established outside the Union

Distributor

Make available on the Union market

KPMG

Cybersecurity and Data Protection Obligations for High Risk AI systems

👆 Deployer (user)
🏭 Provider

🟪 Cybersecurity
🟦 Data protection

🏭 🟪 **Design and development with an appropriate level of Cybersecurity**
(Art. 15)

🏭 🟪 **Data Protection Impact Assessment (DPIA)**
(Art. 29(6))

🏭 🟪 **Cybersecurity Risk Assessment, and, if needed, implementation of appropriate Cybersecurity measures**
(Art. 9)

👆 🟦 **Technical documentation on Cybersecurity measures taken**
(Annex IV 2(ga))

Common practices when implementing AI (ethics) Governance

In our experience, there are several aspects that organizations tend to address immediately when they seek to understand and manage the risks associated with AI. While there is a broader spectrum of considerations, we can broadly categorize them into three areas that require particular focus, namely: 1) Policies, 2) Oversight, and 3) Operations.

Policies

1. Definitions

AI ACT

- To enable effective AI (Ethics) governance and control, a clear definition is needed.
- The AI Act sets an appropriate basis.

2. (risk) Classification model

AI ACT

- All organizations work with an AI (risk) classification model, that helps to determine appropriate risk and control measures.
- The AI Act sets an appropriate basis.

3. AI (/Ethics) Guidelines & Policy

AI ACT

- Guidelines are the starting point to translate the companies risk appetite on AI (Ethics) into actionable measures.
- The extend of the guidelines depends on a principle or rule-based approach.

Oversight

4. Council

- All organizations work with a Council to put oversight in place on AI. Typically the members are very senior and represent both business and risk domains.
- Council also focussed on value creation.

5. Council support role(s)

- As the council is in place to make executive decisions, it typically is supported by a technical committee.
- Trusted advisors are typically supporting the business as primary contact.

6. Ex ante and ex post oversight

- Initial focus is on ex ante oversight, approving AI use cases beforehand.
- Council typically also gets involved in ex post reviews and internal control.

Operations

7. AI registry

AI ACT

- All organizations work with an AI registry to ensure that all (impactful) AI are properly identified and monitored.

8. (AI) Impact assessment

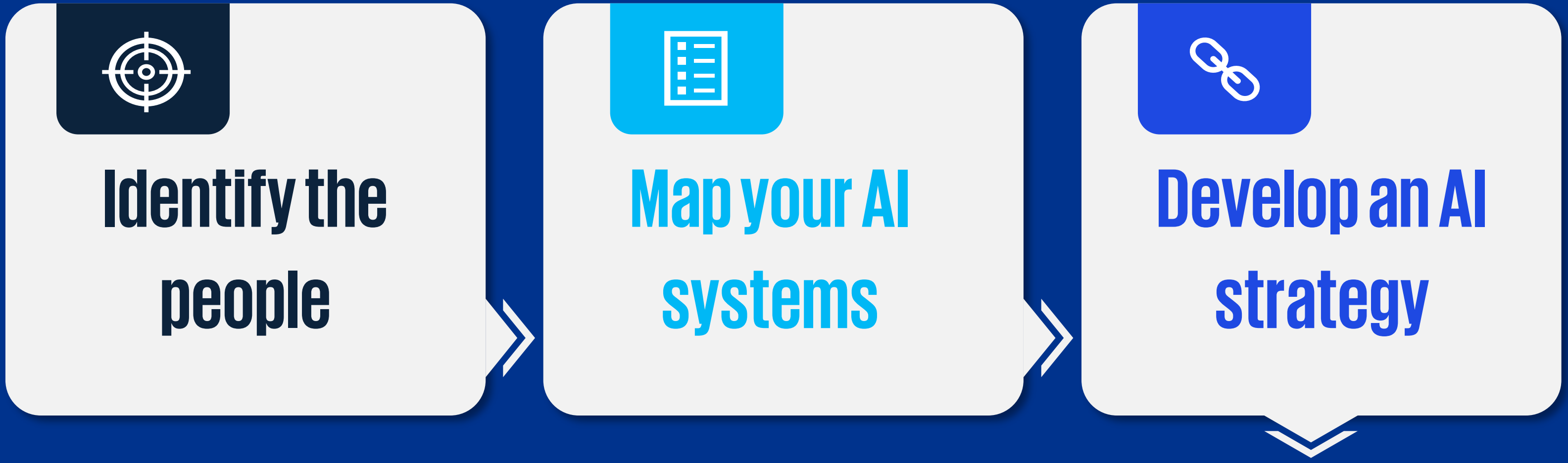
AI ACT

- To operationalize AI (Ethics) governance, all organizations work with risks assessments translating guidelines into actionable questions.

9. Alignment with way of working

- Relevant staff are trained to understand the governance process.
- Technical tools are reviewed to minimize burden on developers and users.

That might be a bit much for now.. so!:

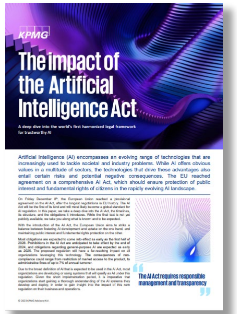


Identify the people

Map your AI systems

Develop an AI strategy

Other questions?



KPMG

The impact of the Artificial Intelligence Act

A deep dive into the world's first harmonized legal framework for trustworthy AI

Artificial Intelligence (AI) encompasses an evolving range of technologies that are increasingly used to tackle societal and industry problems. While AI offers obvious values in a multitude of sectors, the technologies that drive these advantages also entail certain risks and potential negative consequences. The EU reached agreement on a comprehensive AI Act, which should ensure protection of public interest and fundamental rights of citizens in the rapidly evolving AI landscape.

On Friday December 8th, the European Union reached a provisional agreement on the AI Act, after the longest negotiations in EU history. The AI Act will be the first of its kind and will most likely become a global standard for AI regulation. In this paper, we take a deep dive into the AI Act, the timelines, its structure, and the obligations it introduces. While the final text is not yet publicly available, we take you along what is known and to be expected.

With the introduction of the AI Act, the European Union aims to strike a balance between fostering AI development and uptake on the one hand, and maintaining public interest and fundamental rights protection on the other.

Most obligations are expected to come into effect as early as the first half of 2026. Prohibitions in the AI Act are anticipated to take effect by the end of 2024, and obligations regarding general-purpose AI are expected as early as 2025. The proposed regulation will have a far-reaching impact on all organizations leveraging this technology. The consequences of non-compliance could range from restriction of market access to the product, to administrative fines of up to 7% of annual turnover.

Due to the broad definition of AI that is expected to be used in the AI Act, most organizations are developing or using systems that will qualify as AI under this regulation. Given the short implementation period, it is imperative that organizations start gaining a thorough understanding of the AI systems they develop and deploy, in order to gain insight into the impact of this new regulation on their business and operations.

> The AI Act requires responsible management and transparency

© 2023 KPMG Advisory N.V.

SCAN ME

Feel free to reach out

Erik van den Berg

Vandenberg.erik@kpmg.nl
+31 6 5791 5720

Jasper Oomen

Oomen.jasper@kpmg.nl
+31 6 1898 3712