Deloitte.
Legal

The EU AI Act

June 2024

The EU AI Act

Artificial Intelligence in the EU is regulated – the countdown to compliance *begins.*

The EU AI Act enters into force 20 days after publication in the Official Journal.

What is the EU AI Act?

The AI Act is an **EU regulation** which lays down a uniform legal framework for the development, placing on the market, putting into service and use of artificial intelligence (AI) systems, in accordance with Union values. The new legislation is designed to **support innovation** and promote the **uptake of human centric and trustworthy AI**, while **protecting against the harmful effects** of AI systems by ensuring a high level of protection of health, safety, and fundamental rights, including democracy, the rule of law and environment.

The AI Act creates a **new regulatory framework**, which will not only create conditions to enter and remain in the market but will also have significant impact on the reputation and positioning, competition, and associated opportunities, as well as operation and liabilities of companies developing or using AI.

What and whom does it apply to?

The EU aligned its **definition** of AI with the recent OECD definition, to mean a machine-based system that is 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 **scope** of the Act extends to providers, users, importers, and distributors of AI systems within the EU, EU users consuming AI systems irrespective of their origins, and non-EU providers or users whose outputs are consumed within the EU.

The EU AI Act

The EU is not the only one regulating AI.

Key elements of the EU AI Act and related instruments in other countries:

GOALS

AI systems on the Union market are safe, secure, and respect fundamental rights and Union values.

FRAMEWORK

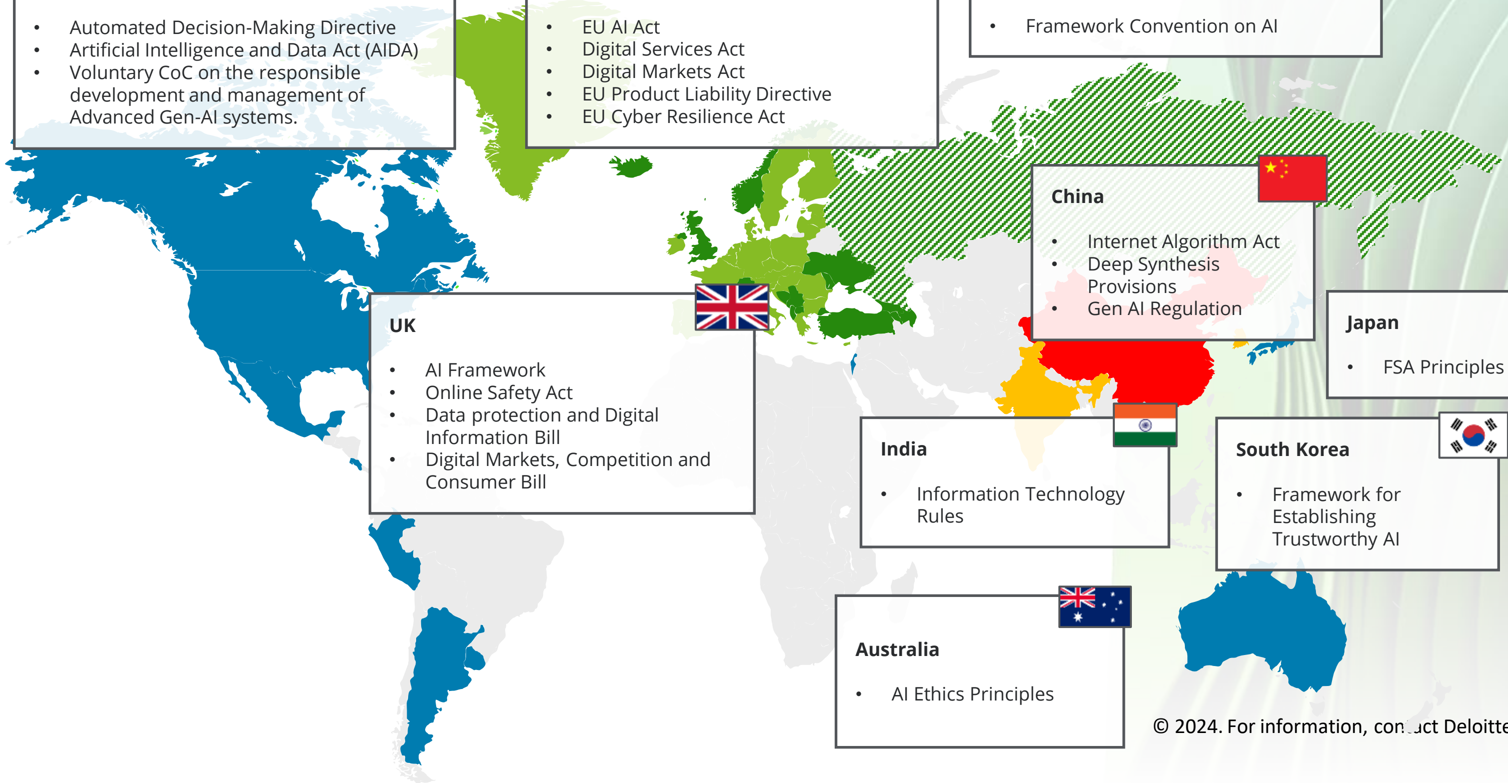
Governance and effective enforcement of requirements applicable to AI systems.

RULES

Foster innovation and investment in safe and trustworthy AI.

MARKET

A level playing field in the EU single market.



USA – Federal

- Algo Accountability Act
- Commercial Facial Recognition Act
- FTC Act
- AI Bill of Rights
- Executive Order on the Safe, Secure and Trustworthy development and use of AI.

USA – State

- Auditing automated hiring tools law (NY)
- Workplace Technology Accountability Act (CA)
- CDOI Regulation Act for Insurers (CO)

Canada

- Automated Decision-Making Directive
- Artificial Intelligence and Data Act (AIDA)
- Voluntary CoC on the responsible development and management of Advanced Gen-AI systems.

European Union

- EU AI Act
- Digital Services Act
- Digital Markets Act
- EU Product Liability Directive
- EU Cyber Resilience Act

Council of Europe

- Framework Convention on AI

UK

- AI Framework
- Online Safety Act
- Data protection and Digital Information Bill
- Digital Markets, Competition and Consumer Bill

China

- Internet Algorithm Act
- Deep Synthesis Provisions
- Gen AI Regulation

Japan

- FSA Principles for MRM

India

- Information Technology Rules

South Korea

- Framework for Establishing Trustworthy AI

Singapore

- AI Model Governance Framework

Australia

- AI Ethics Principles

What approach has been taken?

The development and use of AI were already subject to various legal and regulatory obligations, including data protection and liability. The AI Act harmonizes some of the existing approaches and creates specific requirements for high-risk AI systems and obligations for their operators.

High-risk systems include various forms of biometrics, the AI use in the field of employment, education, critical infrastructure, provision of essential services, or in activities related to law enforcement, border control, judiciary, and democratic processes. AI systems in these cases will **not be considered high-risk** if they do not pose a significant risk of harm to the health, safety, or fundamental rights of natural persons, for example when they do not materially influence the outcome of decision making, to which providers will need to conduct and document a prior assessment and register with the authorities. Similarly, the AI Act provisions will apply to the **existing product safety legislation** which already requires certification of products such as medical products, industrial machinery, or toys.

Some types of use are considered unacceptable by the AI Act and will become prohibited in 6 months. They include AI systems used for exploitation of persons' vulnerabilities, subliminal techniques aimed at distorting behavior of persons, social scoring, predictive policing, real-time biometric identification by law enforcement, biometric classification on sensitive characteristics or inference of emotions in certain situations.

Certain systems which are intended to interact directly with natural persons will need to adequately inform them that they are interacting with an AI system. Similarly, deployers of emotion recognition or biometric categorization systems will need to inform the natural persons who are exposed to the operation of such systems.

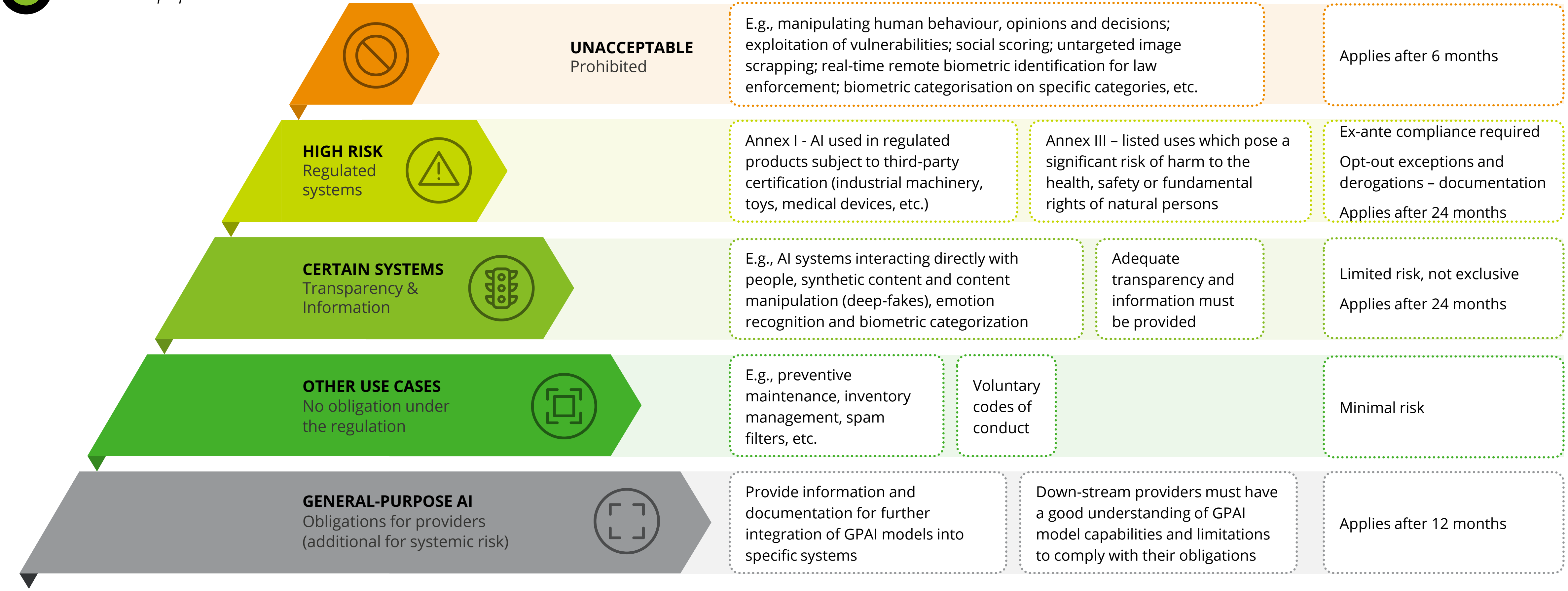
Systems which generate synthetic content will need to ensure that the outputs are marked in a machine-readable format and detectable as artificially generated or manipulated, and disclosure will also be required by the deployers of AI systems which generates deep fakes. In some cases, obligations regarding certain systems will overlap with obligations regarding high-risk cases.

The AI Act also addresses the obligations for providers of general-purpose AI models, who will need to prepare and maintain the technical documentation of the model and provide information and documentation to down-stream providers who intend to integrate the models into their AI systems, so that they have a good understanding of the capabilities and limitations. Providers will also need to comply with copyright and related rights, and adequately disclose the content used for training of the models. Additionally, some GPAI models with high impact capabilities will be classified with systemic risk.

Risk-based and proportionate

The development and use of new technologies will be subjected to a risk-based and proportionate approach, and the new requirements will apply to all actors along the AI value chain and lifecycle, including developers and users.

Risk-based and proportionate



UNACCEPTABLE
Prohibited

E.g., manipulating human behaviour, opinions and decisions; exploitation of vulnerabilities; social scoring; untargeted image scrapping; real-time remote biometric identification for law enforcement; biometric categorisation on specific categories, etc.

Applies after 6 months

HIGH RISK
Regulated systems

Annex I - AI used in regulated products subject to third-party certification (industrial machinery, toys, medical devices, etc.)

Annex III – listed uses which pose a significant risk of harm to the health, safety or fundamental rights of natural persons

Ex-ante compliance required

Opt-out exceptions and derogations – documentation

Applies after 24 months

CERTAIN SYSTEMS
Transparency & Information

E.g., AI systems interacting directly with people, synthetic content and content manipulation (deep-fakes), emotion recognition and biometric categorization

Adequate transparency and information must be provided

Limited risk, not exclusive

Applies after 24 months

OTHER USE CASES
No obligation under the regulation

E.g., preventive maintenance, inventory management, spam filters, etc.

Voluntary codes of conduct

Minimal risk

GENERAL-PURPOSE AI
Obligations for providers (additional for systemic risk)

Provide information and documentation for further integration of GPAI models into specific systems

Down-stream providers must have a good understanding of GPAI model capabilities and limitations to comply with their obligations

Applies after 12 months

How will it affect companies?

Compliance with the AI Act will be a condition for the placing of AI systems on the market, their putting into service or use.

For high-risk uses, **the providers** will need to establish quality management systems, including risk management, and prepare adequate technical documentation. Placing of AI products on the market will require an ex-ante conformity assessment, registration and CE marking, and post-market activities such as monitoring, corrective actions, information duty and cooperation with the authorities. AI systems will, among other obligations, need to be designed and developed to achieve appropriate levels of accuracy, robustness, and cybersecurity, and perform consistently throughout their lifecycles. Development will require appropriate data governance and management practices, including regarding data collection, the formulation of assumptions, and examination of possible biases. Sufficient transparency will need to be ensured by instructions for use to enable deployers to interpret a systems' output and use it appropriately.

The deployers will need to take appropriate technical and organizational measures to ensure the use of the systems in accordance with the instructions, and assign human oversight with necessary training, competence, and authority. The use will require monitoring and logging, and in some cases, deployers will need to conduct preliminary fundamental rights impact assessments.

To minimize the burden on operators, most of **conformity assessments** can be performed internally. However, where market surveillance authorities have sufficient reason to consider that the systems classified by the provider as non-high-risk are indeed high-risk, they will be enabled to carry out evaluations, require appropriate corrective actions or issue fines. Providers of AI systems that are not high-risk are therefore encouraged to create codes of conduct, including related governance mechanisms.

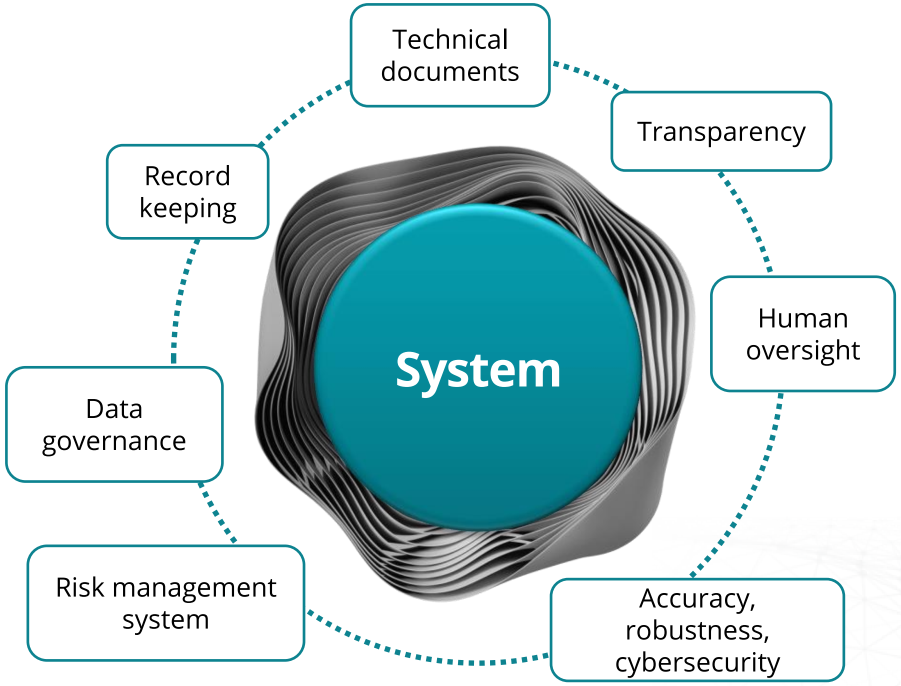
Non-compliance will be subject to **enforcement and significant penalties,** including fines and recall or withdrawal from the market. Use of prohibited systems can result in administrative fines of up to EUR 35 million or 7% of the global annual turnover, while other infringements are set at EUR 15 million or 3% of the global annual turnover. The supply of incorrect, incomplete, or misleading information to authorities can be subject to fines of EUR 7.5 million or 1% of the global annual turnover.

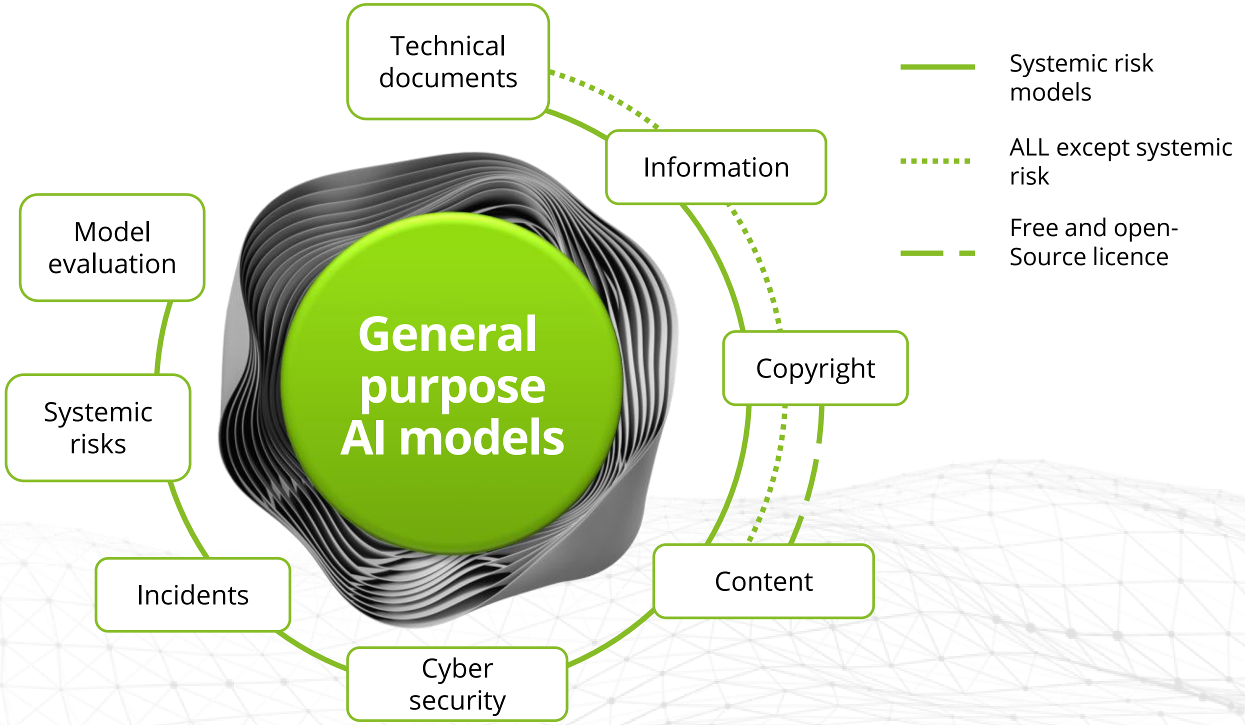
Enforcement and penalties

Prohibited practices	Other non-compliance	Incorrect, incomplete or misleading
<35 MIO EUR or 7%	<15 MIO EUR or 3%	<7.5 MIO EUR or 1%

What will be the requirements?

AI Act is overall tech-neutral and future-proof, but uses quantitative benchmarks for presumption of high-impact capabilities of GPAI models.





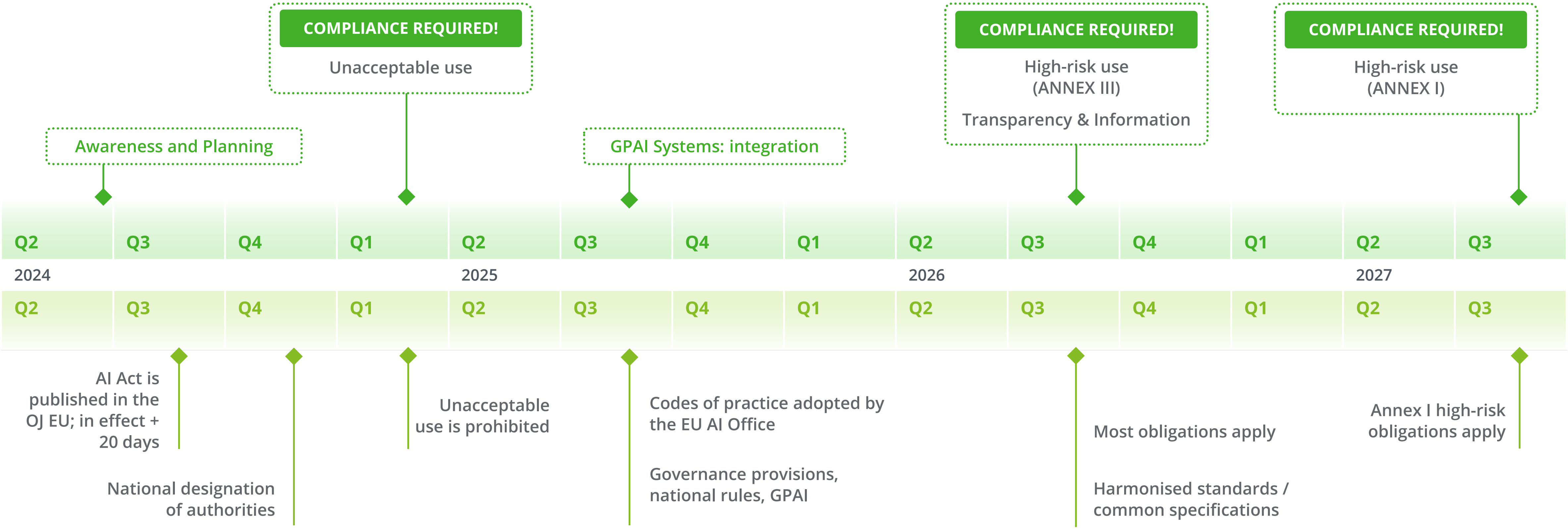
What is the timeline?

The AI Act enters into force 20 days after its publication in the Official Journal of the European Union. While compliance with most of the requirements will be needed in 24 months, important provisions related to unacceptable use will become effective already in 6 months.

Providers of general-purpose AI models and systems will need to comply with the AI Act within 12 months, to allow down-stream developers and deployers to achieve compliance in their specific solutions.

Providers of high-risk AI systems are encouraged to start to comply, on a voluntary basis, with the relevant obligations of the AI Act already during the transitional period.

EU AI Act Timeline



Awareness and Planning

COMPLIANCE REQUIRED!

Unacceptable use

GPAI Systems: integration

COMPLIANCE REQUIRED!

High-risk use (ANNEX III)

Transparency & Information

COMPLIANCE REQUIRED!

High-risk use (ANNEX I)

Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
2024				2025				2026				2027	

AI Act is published in the OJ EU; in effect + 20 days

National designation of authorities

Unacceptable use is prohibited

Codes of practice adopted by the EU AI Office

Governance provisions, national rules, GPAI

Most obligations apply

Harmonised standards / common specifications

Annex I high-risk obligations apply

What are the steps towards compliance?

The transition period requires AI system deployers to identify the AI systems they are using and assess their conformity without further delay to prevent potential non-compliance.

The first steps should often be aimed at identification and classification of all AI systems that are being used in the work processes, and their assessment towards compliance with the AI Act requirements.

Providers and deployers are encouraged to analyze the potential gaps in their overall development and implementation of the technology and define their path towards target operating models. This includes development of general quality and risk management systems, policies for data governance and management, and ensuring sufficient levels of AI literacy of staff and other persons, and preparation of adequate technical documentation and user instructions for specific systems.

Steps towards compliance

Steps towards compliance

Post-market monitoring

Internal and external compliance requirements throughout life cycle

Re-assessment

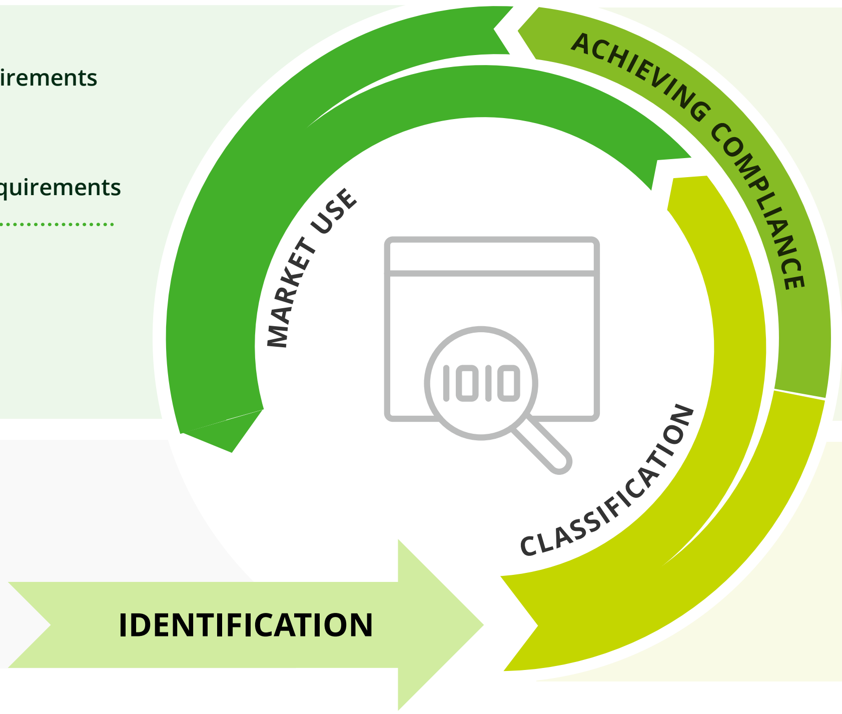
Due to substantial modifications or requirements

→ Human oversight

→ Record-keeping

→ Cooperation with authorities

→ Examine existing or planned systems to determine if they qualify as AI under AI Act



Implementing relevant AI Act requirements

- Quality and risk management, data governance, documentation, transparency, accuracy, oversight, etc.
- Conformity assessment

Declaration of conformity

Affix CE marking after establishing compliance

Registration

- EU database to increase public transparency and oversight
- National registration for critical infrastructure

→ Mapping of products and roles

→ Risk and impact assessment

→ Determination of requirements

How can Deloitte help?

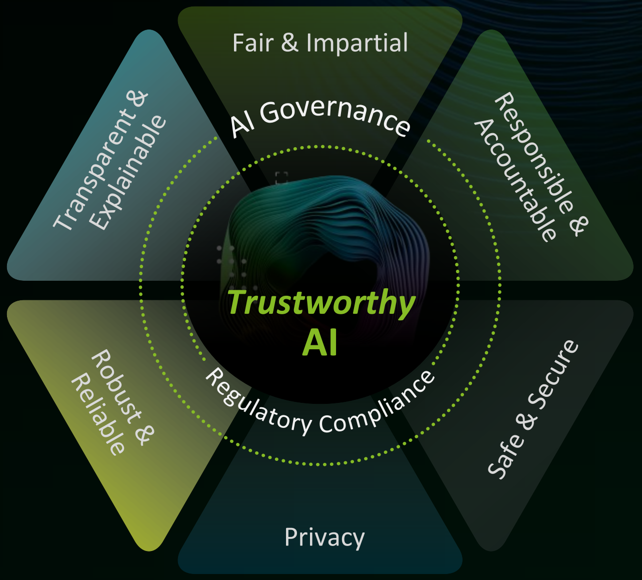
To prevent blind spots during the initial steps, or to find optimal solutions at other stages of the process, compliance activities benefit from a holistic approach.

Through its multidimensional Trustworthy AI Framework, Deloitte helps organizations develop safeguards for trustworthy AI development and deployment at all levels of the supply chain.

Our multidisciplinary capabilities in legal, risk, ethics, audit, assurance, business, and technology consulting enable tailored, efficient, and effective support through all lifecycle stages of AI systems, on a global level and with an in-depth understanding of local specifics.

Deloitte's experience ranges from high-level AI governance and improving operations to providing support for regulatory activities to access the markets and supply-chain alignment for specific applications. We assist clients in bridging gaps, developing specific solutions, or assessing the value of proposals and implementations.

Deloitte's Trustworthy AI Framework



Get in touch

Contact us now

to find out more about this legislation and how we can support you in your AI journey.

CENTRAL EUROPE REGIONAL LEADS

Jan Michalski

Partner, Central Europe GenAI Leader

E: jmichalski@deloittece.com

Simina Mut

Partner, Deloitte Legal Central Europe Leader

E: smut@deloittece.com

Gregor Strojin

Deloitte Legal Central Europe AI Regulatory CoE Leader

E: gstrojin@deloittece.com

ALBANIA

Ina Cota
Manager

icota@deloittece.com

Ened Topi
Senior Manager, Deloitte Legal

etopi@deloittece.com

BOSNIA & HERZEGOVINA

Elma Delalic-Haskovic
Manager

edelalic@deloittece.com

Zerina Pacariz
Manager

zpacariz@deloittece.com

BULGARIA

Mila Goranova
Senior Consultant

mgoranova@deloittece.com

Adelina Mitkova
Senior Manager, Deloitte Legal

amitkova@deloittece.com

CROATIA

Zrinka Vrtarić
Attorney at law in cooperation with Deloitte Legal

zvrtaric@kip-legal.hr

Ratko Drča
Director

rdrca@deloittece.com

CZECH REPUBLIC

Jaroslava Kracunova
Partner, Deloitte Legal

jkracunova@deloittece.com

Jakub Holl
Director

jholl@deloittece.com

ESTONIA, LATVIA, LITHUANIA

Maksims Naumovs
Data Modernization and Analytics Offering Lead at Deloitte Central Europe, AI & Data Director

mnaumovs@deloittece.com

Romans Taranovs
AI & Data Director

rtaranovs@deloittece.com

© 2024. For information, contact Deloitte Legal Central Europe.

HUNGARY

Lili Albert
Senior Associate, Deloitte Legal

lialbert@deloittece.com

Gergő Barta
Senior Manager AI Risk & Compliance

gbarta@deloittece.com

KOSOVO

Ardian Rexha
Senior Manager, Deloitte Legal

arudi@deloittece.com

Donika Ahmeti
Senior Manager

gbarta@deloittece.com

POLAND

Mateusz Ordyk
Partner, Deloitte Legal

mordyk@deloittece.com

Scibor Lapies
Partner

slapies@deloittece.com

ROMANIA

Simina Mut
Partner, Deloitte Legal Central Europe Leader

smut@deloittece.com

Andrei Paraschiv
Partner

anparaschiv@deloittece.com

SERBIA

Stefan Ivic
Partner

stivic@deloittece.com

Miroslava Gaćeša
Director

mgacesa@deloitteCE.com

SLOVAKIA

Dagmar Yoder
Partner, Deloitte Legal

dyoder@deloittece.com

Pavol Szabo
Senior Managing Associate, Deloitte Legal

pszabo@deloittece.com

SLOVENIA

Ana Kastelec
Attorney at law, Local Partner in Law Firm Deloitte Legal Reff – Branch in Slovenia

akastelec@deloittece.com

Lan Filipič
Director

lfilipic@deloittece.com

UKRAINE

Dmytro Pavlenko
Partner

dpavlenko@deloittece.com

Mykhailo Koliadintsev
Legal Managing Associate

mkoliadintsev@deloittece.com

Deloitte.
Legal

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Legal means the legal practices of DTTL member firms, their affiliates or their related entities that provide legal services. The exact nature of these relationships and provision of legal services differs by jurisdiction, to allow compliance with local laws and professional regulations. Each Deloitte Legal practice is legally separate and independent, and cannot obligate any other Deloitte Legal practice. Each Deloitte Legal practice is liable only for its own acts and omissions, and not those of other Deloitte Legal practices. For legal, regulatory and other reasons, not all member firms, their affiliates or their related entities provide legal services or are associated with Deloitte Legal practices.

Deloitte Central Europe is a regional organization of entities organized under the umbrella of Deloitte Central Europe Holdings Limited, a 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 13,000 people in 45 offices in 19 geographies.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.