AI ACT

Walk-Through

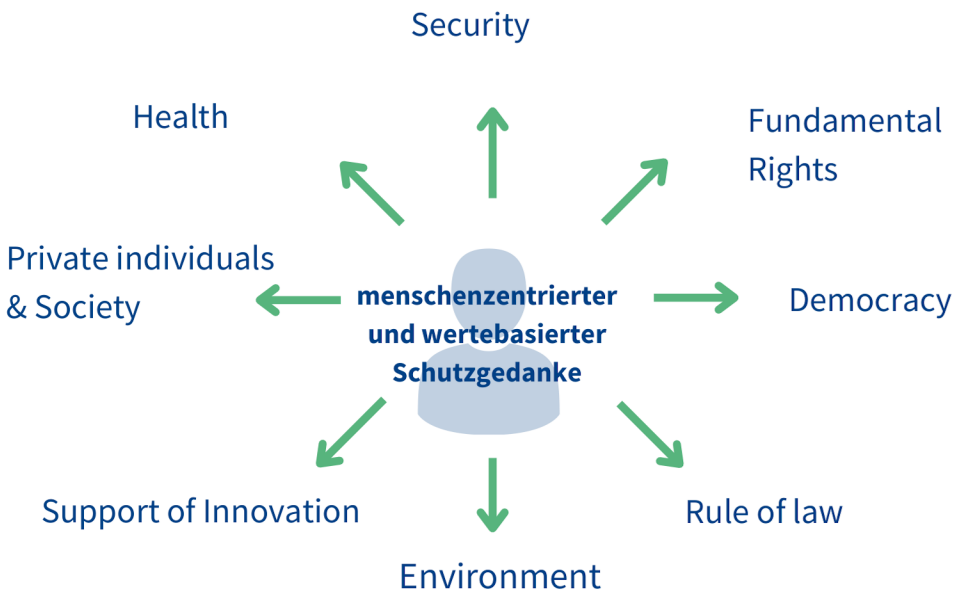
DORDA

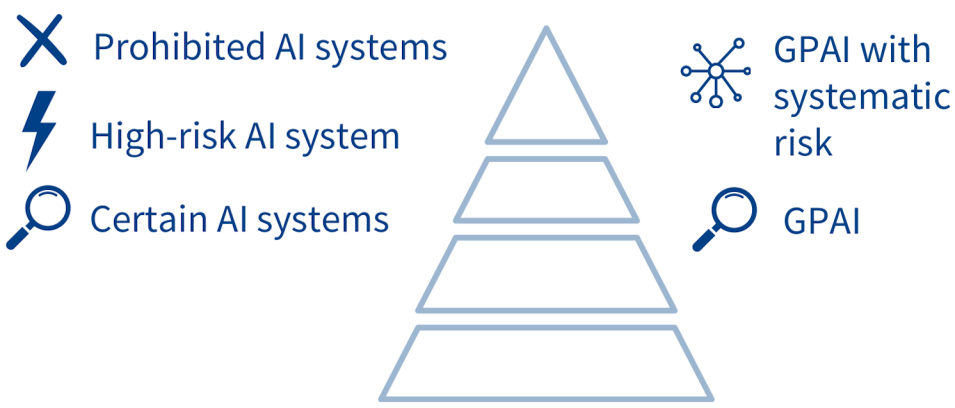
| Digital Industries Group |

Overview

Objectives

The AI Act creates a legal framework for safe and trustworthy use of AI systems in the EU. At the same time, it aims to foster innovation.





Centrepiece of the AI Act: The risk-based approach

The AI Act qualifies AI considering its risks by a classification system. Depending on the categorisation, the use of an AI system is subject to different obligations. General purpose AI (GPAI) is specifically regulated.

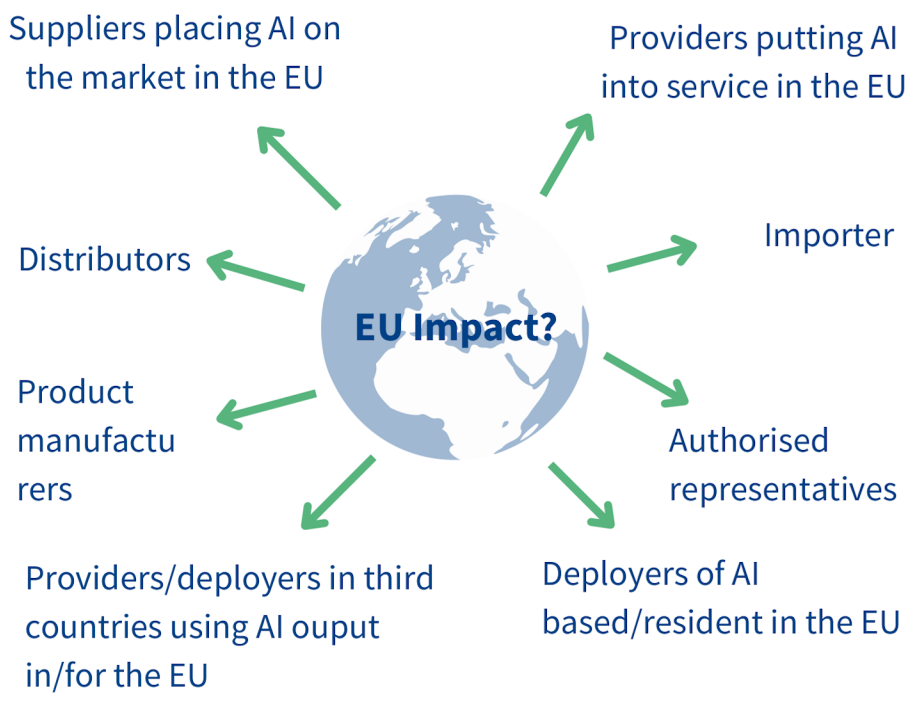
Good News! All AI systems that do not fall into one of these risk categories will be permitted under the AI Act without further measures.

Obliged parties

The AI Act put obligations on various players:

- Providers
- Deployers
- Importers and distributors
- Product manufacturers
- Authorised representatives of providers

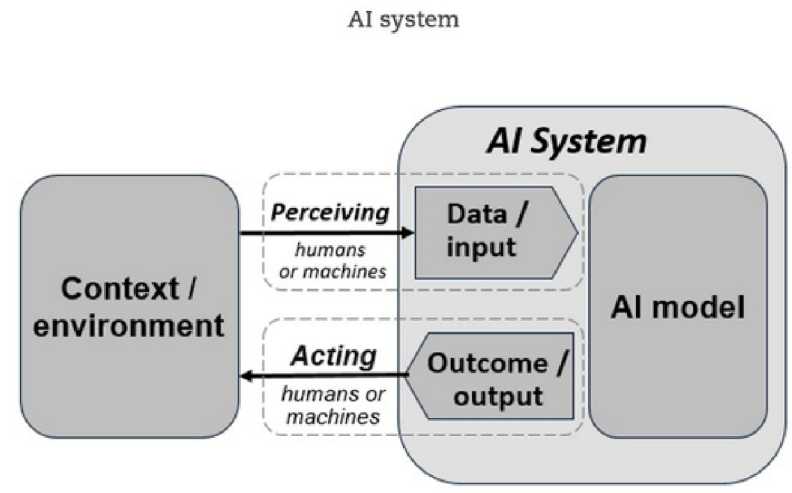
A registered office in a third country does not release the actors from their obligations if the AI system is intended for usage in the EU.



How-To AI Act-Compliance?

Step 1: Is my system qualified as AI under the AI Act?

Parallels to the OECD definition



https://oecd.ai/en/ai-principles

KI-Definition

"AI-System" means a machine-based system that is

- designed to operate with varying degrees of autonomy,
- may exhibit adaptiveness after its deployment,
- interfers from the input received based on explicit or implicit objectives how the output may influence the physical or virtual environments.

Such output are for example predictions, content, recommendations or decisions influencing the environments they interact with.

Increases international convergence and acceptance

Definition of GPAI

"General-purpose AI system" means an AI model that

- displays significant generality,
- is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market, and
- can be integrated into a variety of downstream systems or applications.

Exceptions: Models for research, development or prototyping activities.

How to distinguish AI from simpler traditional software?

Key characteristics of AI:

- Capability to infer to the process of obtaining outputs
- Use of techniques such as machine learning, logic and knowledge-based approaches
- Systems with varying degrees of autonomy

Not covered:

- Software based solely on rules defined by natural persons for the automatic execution of operations

Beispiele

AI systems may be integrated into the following applications (to be checked on a case-by-case basis):

- Spam filters
- Chatbots, voicebots
- Tools for the automated evaluation of applications, processing of customer enquiries, applications, processing of contracts, etc
- Robot-assisted devices, such as in medicine
- Credit scoring systems
- Sensor-assisted systems, such as in road traffic

Practical advice

Examine whether AI systems, as defined by the AI Act, are already in use and consider the applicability of the AI Act for new use cases.

Step 2: Does the use of my AI fall within the scope of the AI Act?

Exceptions to the scope of application

- Use for **military purposes** only
- Use for **defence** or **national security** purposes
- Use of AI specifically developed and put into service for the sole purpose of **scientific research and development**
- **Research, tsting and development activities** prior to placing AI on the market or put into services, unless carried out under real world conditions
- Use by natural persons for **purley personal and non-professional** actvities
- Provision under **free and open source licences**

However, AI systems that are made available under free and open source licences must **not constitute prohibited AI systems.** If these AI systems fall into the **high-risk category**, the obligations and requirements of the AI Act must be ahrered anyways.

More information on the **classification under step 4**

Practical advice

The requirements for each exemption must be carefully considered on a case-by-case basis and be interpreted strictly.

Step 3: In which role do I use AI?

A matter for the entire supply chain

The obligations and prohibitions of the AI Act are primarily aimed at **providers/deployers of AI solutions**. This is anyone who **develops AI**, **has it developed**, **places it on the market** or **puts it into operation** under his own name. In order to avoid a gap in legal protection, **other market participants** are also subject to the same obligations. The legal framework of the AI Act is therefore relevant for the entire supply chain - **from the manufacturer to the end user**.

Provider

Manufacturer and distributor under their own brand

Importer

Importer from a third country into the EU with an establishment in the EU

Distributor

Suppliers in the EU market

Deployer

Use under own responsibility

Practical advice

Activities set by other parties than traditional service providers may also be covered by the AI Act. Compliance risks can be identified and mitigated at an early stage by assessing the scope of applicability of the AI Act.

Step 4: How is the AI system classified and which obligations must be met?

Verbotene KI-Systeme

In particular, this includes AI systems for one or more of the following purposes

- Materially distorting the of persons by manipulative techniques
- Social scoring
- Automated facial recognition for the sole expansion of databases thorugh scraping
- Real-time biometric identification

Prohibited AI systems **must not be placed on the market or used in the EU.**

There are only **limited exceptions**, notably for law enforcement. The use of facial recognition systems and real-time biometric identification is allowed under certain conditions.

Partial derogation by risk assessmentby risk assessment

However, the AI Systems listed in Annex III shall 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, including by not materially influencing the outcome of the decision making. This risk assessment must be carried out in accordance with the parameters set out in the AI Act.

High-risk AI systems

This includes AI systems that

- are used as a safety components and fall under the regulations listed in **Annex I of the AI Act** (eg the Directive on the safety of toys or lifts),
- are listed in **Annex III of the AI Act** (eg certain biometric applications, AI in critical infrastructure, education and training, certain AI systems in HR, credit scoring, risk assessment and pricing in the case of health and life insurance).

Obligations

High-risk AI systems can only be placed on the market and used in the EU if specific requirements are met, such as:

- Establishment and maintenance of a risk management system, in particular carrying out an AI risk assessment
- Fundamental rights impact assessment for Annex III applications
- Compliance with data quality requirements
- Technical documentation requirements
- Record-keeping obligations
- Transparency obligations
- Human oversight
- Ensuring accuracy, robustness and cybersecurity

In addition, providers must have an EU Declaration of Conformity and affix a CE marking. Details are set out in Section 2 et seq of the AI Act and its Annexes.

Practical advice

The focus in AI compliance projects should be on the high-risk classification. This classification carries the most obligations and should be prioritised. The Commission will issue guidance on the practical implementation of high-risk AI and provide a list of examples of such AI systems no later than 18 months after entry into force. However, given the 24-month implementation period, waiting for the guidance is very risky.

Obligations

Certain AI systems may pose a particular risk of identity fraud or deception. They are therefore primarily subject to **transparency rules.**

Certain AI systems

These include, for example, AI systems that were developed to interact with people (classic chatbots) or to generate content.

GPAI

GPAI is characterised by the fact that these models can be used for **different purposes** due to their **performance and scope**. The developer does not determine the actual use by enduser.

With a computing power of more than **10^25 FLOPS**, AI models are basically qualified as a **systemic risk model**.

Obligations

All GPAI providers must adequately document the system development and **training content** and also provide appropriate **information to downstream providers** so that they can understand the system. This includes:

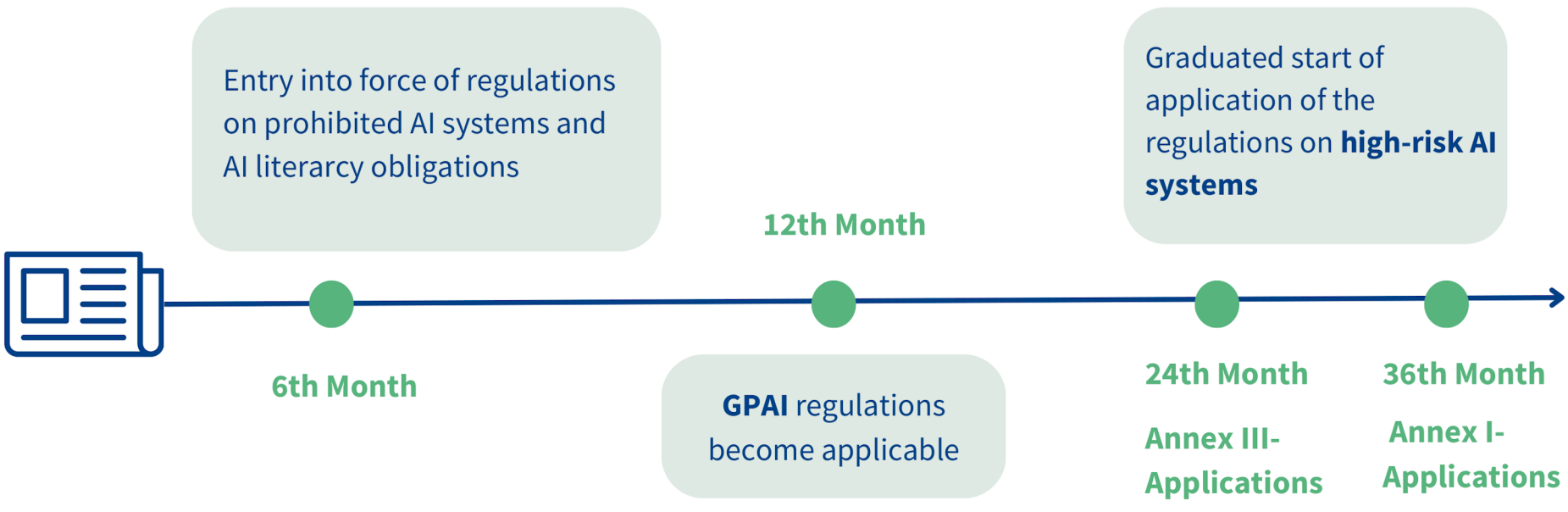
- Disclosing that the content was generated by AI
- Preventing the generation of illegal content through appropriate product design
- Publication of general summaries of copyrighted content used for training purposes

Providers of GPAI with **systemic risks** must also carry out a **model assessment** of possible risks, meet certain **reporting** obligations and ensure **cybersecurity measures.**

Special rules apply to developers and providers of free and open source software.

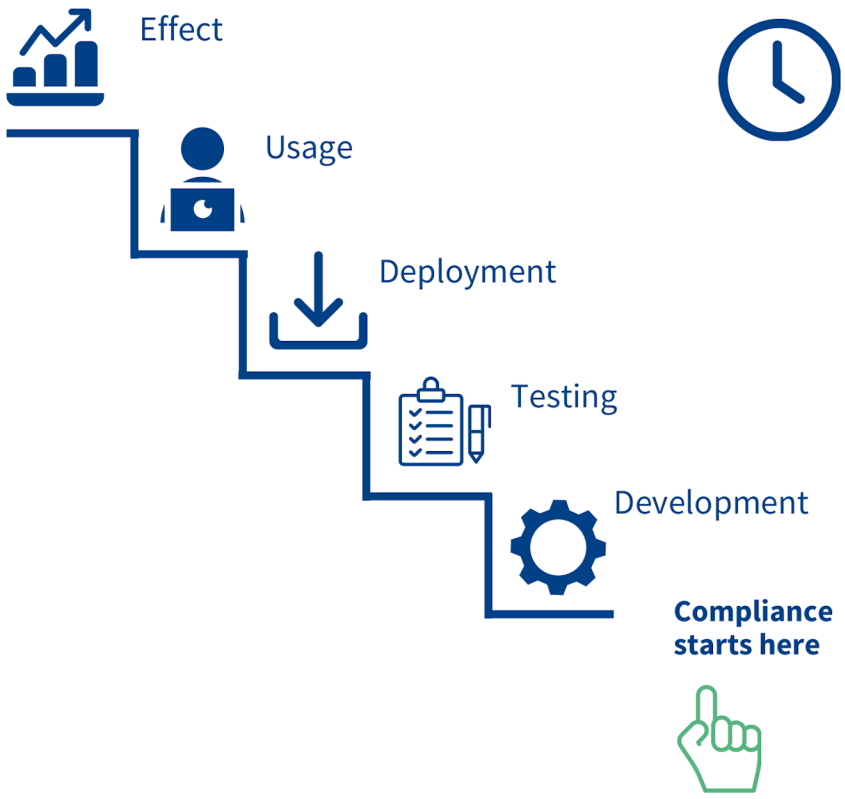
Step 5: Implementation of AI Act obligations on time

Wichtige Compliance Fristen



The **provisions of the AI Act** will **gradually** come into effect for affected persons after the Act **comes into force.**

In order to ensure the legally compliant use of current AI systems or those under development, it is advisable **to take appropriate compliance measures now.** Otherwise, there is a risk that a lack of preparation will prevent the necessary obligations from being met in good time. This could result in severe **penalties**.



Fines

Breach of provisions on **prohibited AI systems** and **data governance**	up to **EUR 35 million** or **7%** of the annual turnover	The **fine is limited** to the lump sum or percentage, **whichever is higher.**
Breach of **general compliance obligations** and **GPAI provisions**	up to **EUR 15 million** or **3%** of the annual turnover	A special rule applies to **SMEs and start-ups.** Here, the **lower amount is used for the maximum fine.**
False statements to the competent authority in AI proceedings	up to **EUR 7.5 million** or **1%** of the annual turnover	

Innovation partner for digital Champions.

Axel Anderl
Managing Partner
Head of IT/IP/Datenschutz
Head of Digital Industries Group

axel.anderl@dorda.at

Alexandra Ciarnau
Co-Head of Digital Industries Group
Rechtsanwältin IT/IP/Datenschutz
Head of Metaverse
Board Member of Women in AI Austria

alexandra.ciarnau@dorda.at

Benjamin Kraudinger
Rechtsanwaltsanwärter
IT/IP/Datenschutz
Digital Industries Group

benjamin.kraudinger@dorda.at