AI ACT

Walk-Through

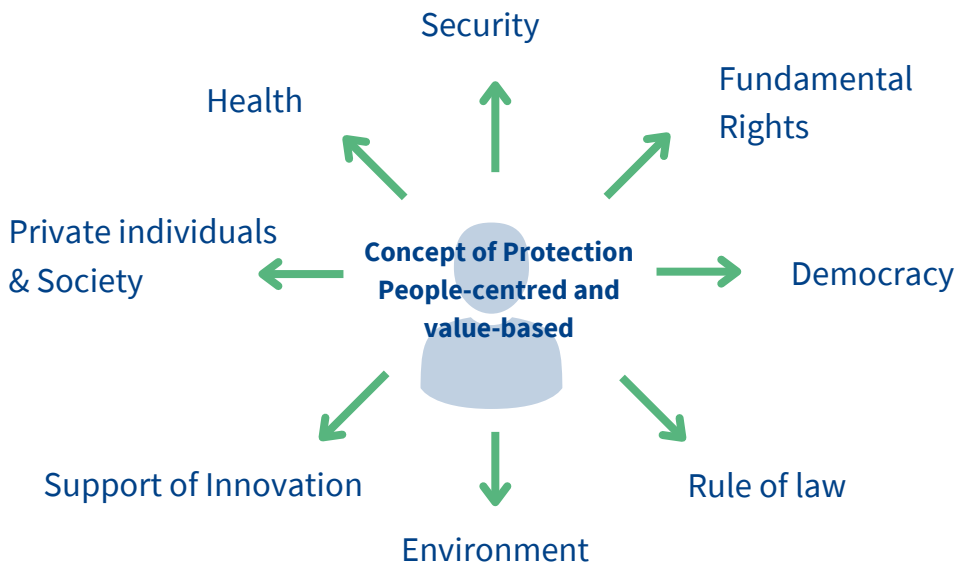
DORDA

| Digital Industries Group |

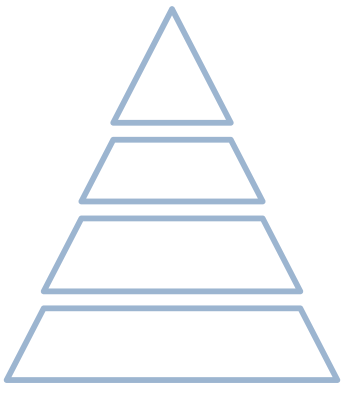
Overview

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.



- Prohibited AI systems
- High-risk AI system
- GPAI
- Certain AI systems



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.

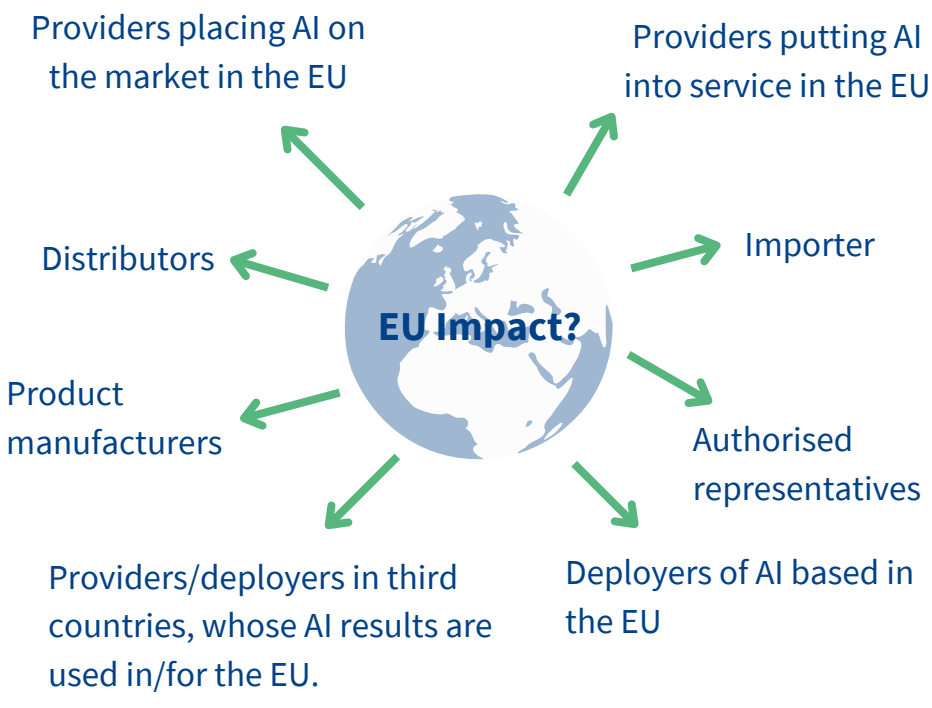
Good News! All AI systems that do not fall into one of these risk classes are permitted under the AI Act without further requirements. For these, only the provisions on **AI literacy** must be observed. In future, all providers and deployers of AI systems will have to take measures to impart the necessary knowledge for the **informed use of AI systems**.

Obliged parties

The AI Act puts obligations on various players:

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

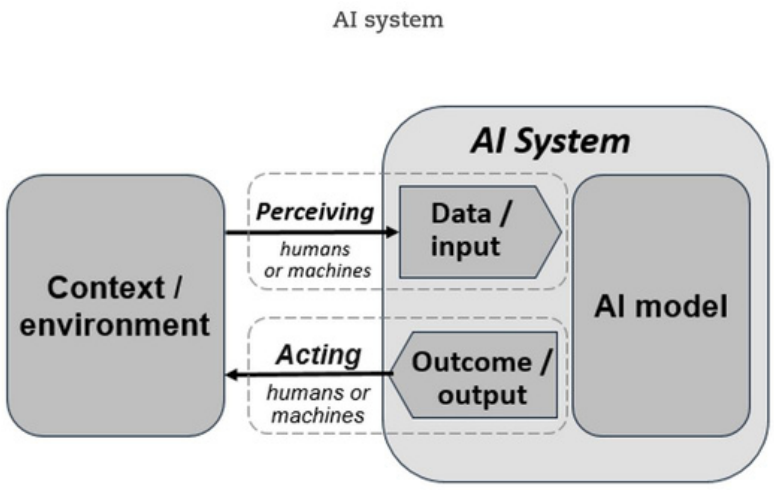
A registered office in a third country does not release the parties from their obligations if the AI is intended for usage in the EU.



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**,
- **infers from the input received**, for implicit or explicit objectives, how to generate **outputs, that can influence physical or virtual environments**.

Such outputs are for example predictions, content, recommendations or decisions.

Increases international convergence and acceptance

Definition of GPAI

"**General-purpose AI model**" 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.

Use Cases

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

How to distinguish AI from simpler traditional software?

Key characteristics of AI:

- Capability to infer from input or data
- 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

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, testing 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**

Practical advice

The requirements for each exemption must be carefully considered on a case-by-case basis and be interpreted strictly. For the private sector, the exceptions for open source software and testing/development activities are the most relevant.

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 the **provider of AI solutions**. This is anyone who **develops AI** or **has it developed** and **places it on the market** or **puts it into operation** under the **own name**. In order to avoid a gap in legal protection, **other market participants** can also be 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 established in the EU that imports AI from a third country into 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?

Prohibited AI systems

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

- AI systems that use techniques of subliminal influence beyond a person's consciousness or purposefully manipulative or deceptive techniques to materially distort the behaviour of a person/group and interfere with decision-making in such a way that significant harm is/can be caused
- Social scoring of individuals
- Real-time biometric identification in publicly accessible spaces outside the narrow scope of exceptions

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 possible by risk assessment

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.

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 Chapter 2 et seq of the AI Act and its Annexes.

High-risk AI systems

This includes AI systems that

- are used as 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) or are themselves considered to be such a regulated product,
- are listed in **Annex III of the AI Act**, in particular in relation to biometric applications, critical infrastructure, education and training, employment, human resource management, access to and use of essential private and public services (in particular AI systems for credit scoring that go beyond the detection of financial fraud), law enforcement, migration, asylum, border control, administration of justice and democratic processes.

Details can be found in Annexes I and III.

Practical advice

The focus in AI compliance projects should be on the high-risk class since this classification carries most of the obligations

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 the enduser.

With a computing power of more than **10^25 FLOPS**, AI models are generally qualified as **models with systemic risks**.

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:

- Information on the functions and limitations of the GPAI model
- Implementation of a EU-copyright compliance strategy
- Summaries of the content used for the training

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

Obligations

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

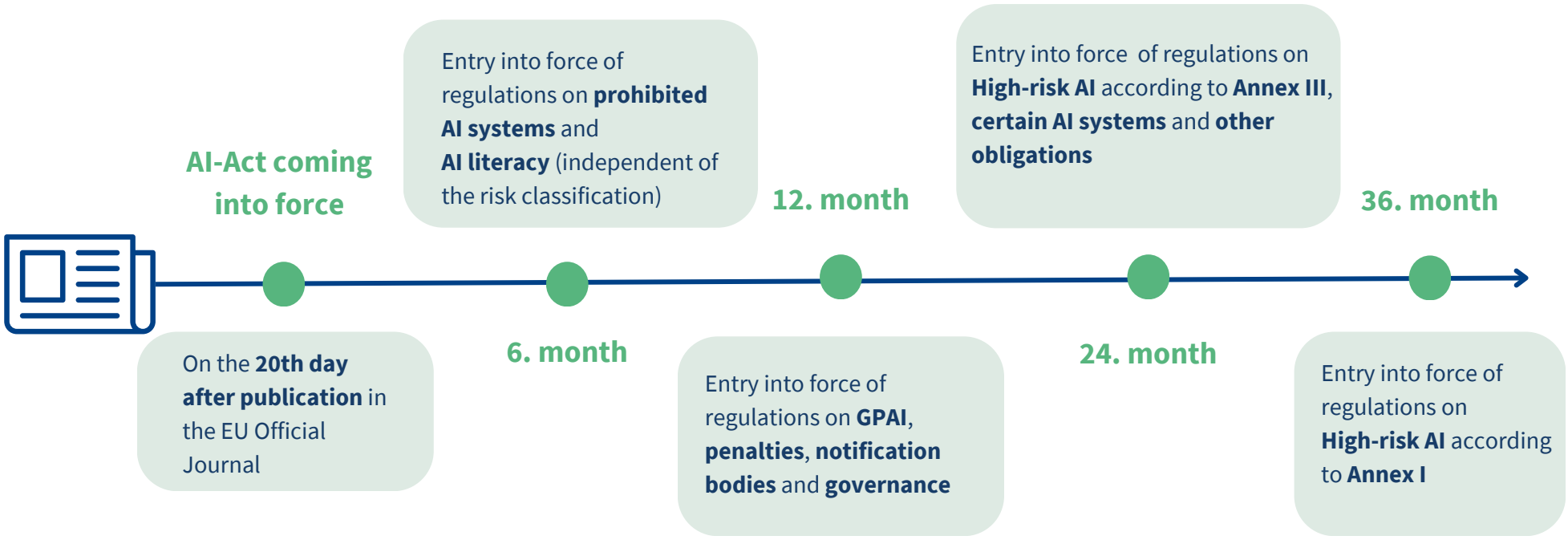
Providers must ensure that **synthetic content** is also recognisable as such and that a user is informed about the **interaction with a machine**. The operator also has a duty to provide information if the generated content is considered a "**deepfake**".

Certain AI systems

These include AI systems that are used for direct interaction with natural persons (classic chatbots) or that generate synthetic audio, image, video or text content. GPAI models are also regularly integrated in this group of AI systems.

Step 5: Implementation of obligations on time

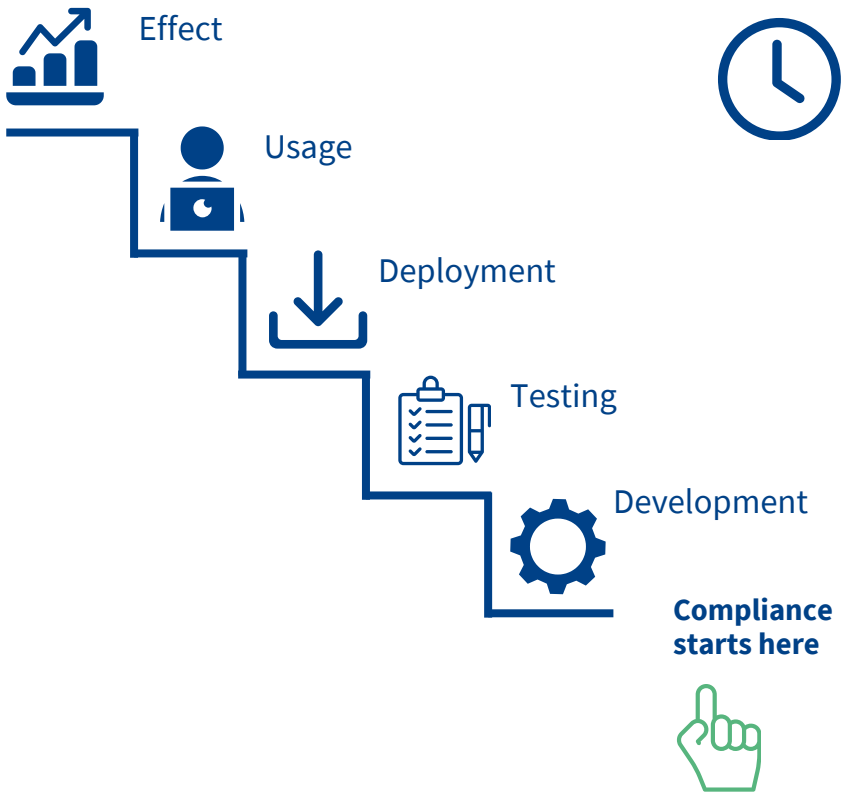
Important Compliance Periods



Different provisions apply in some cases to AI systems that are already on the market or have been put into operation.

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**	up to **EUR 35 million** or **7%** of the annual turnover
Breach of provisions on **High-risk AI systems**, **GPAI provisions** and **transparency obligations for certain AI systems**	up to **EUR 15 million** or **3%** of the annual turnover
False statements to the competent authority in AI proceedings	up to **EUR 7.5 million** or **1%** of the annual turnover

The **fine is limited** to the lump sum or percentage, **whichever is higher.**

A special rule applies to **SMEs and start-ups.** Here, the **lower amount is used for the maximum fine.**

Innovation partner for digital champions.

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

axel.anderl@dorda.at

Alexandra Ciarnau
Principal Associate
IT/IP/Data Protection
Co-Head of Digital Industries Group
Head of Metaverse
Board Member of Women in AI Austria

alexandra.ciarnau@dorda.at

Benjamin Kraudinger
Associate
IT/IP/Data Protection
Member of Digital Industries Group

benjamin.kraudinger@dorda.at