Ministry of Economic Affairs

AI Act Guide

Version 1.1 – September 2025

Cover image: Wes Cockx & Google DeepMind / BetterImages of AI / AI large language models / CC-BY 4.0

Guide to reading this document and disclaimer
You develop AI systems or are considering using them in your organisation. In that case, you may well come into contact with the AI Act. This guide has been prepared as a tool to provide you with easy insight into the key aspects of the AI Act. **No rights may be derived from the content of this guide.** The legal text of the AI Act always takes precedence.

Please submit any feedback on this guide to ai-verordening@minezk.nl. Your feedback will be used to improve future editions of the guide.

If you are reading a paper version of the guide, visit ondernemersplein.nl for the latest version. The website also provides references to the latest guidelines from the European Commission. At the time of publication, guidelines have been issued regarding the definition of AI, prohibited AI and General Purpose AI models.

The AI Act

The AI Act is an extensive legal document governing Artificial Intelligence (AI) for the entire European Union (EU). The AI Act contains rules for the responsible development and use of AI by businesses, government and other organisations. The aim of the regulation is to protect the safety, health and fundamental rights of natural persons. Application of the regulation means that organisations can be certain that the AI they use is responsible and that they can enjoy the benefits and opportunities offered by AI.

The regulation will be introduced in phases and the majority will apply as from mid-2026 onwards. A number of AI systems have already been prohibited since February 2025. Given this situation, it is important that you make the necessary preparations. To help you in that process, this guide lists the most important provisions from the AI Act. However, no rights may be derived from the information contained in this document. Its sole purpose is to provide support. Click here[1] for the complete text of the regulation.

What does the AI Act mean for your organisation?

Depending on the type of AI system and the use to which the organisation puts that system, requirements will be imposed on its development and use. Whether requirements are imposed will among others depend on the risk the AI system represents to safety, health and fundamental rights. Different requirements will be imposed on organisations that develops an AI-system or has it developed than on organisations that make use of AI. To find out what the AI Act means for your organisation, it is important to work through the four steps listed below. These steps are explained further in this guide:

Step 1 (Risk): Is our (AI) system covered by one of the risk categories?
Step 2 (AI): Is our system 'AI' classified according to the AI Act?
Step 3 (Role): Are we the provider or deployer of the AI system?
Step 4 (Obligations): What obligations must we comply with?

Note: Many other guides and step-by-step plans start at step 2 (is our system 'AI') rather than step 1 (risk categories). After all, if an AI system does not qualify as 'AI' there are no requirements subject to the AI Act. However, even for systems which are not categorised as AI according to the AI Act, it is important to have a clear idea of the risks of the purposes for which they are used. That is why in this AI Act Guide, we have chosen to start with the risk categories.

[1] https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32024R1689

Step 1. (Risk) Is our (AI) system covered by one of the risk categories?

All AI systems are subject to the AI Act, but depending on the risk, different requirements are imposed on different categories of system. The risk is determined by the intended application or the product for which the AI system is being developed, sold and used:

- **Prohibited AI practices:** these AI systems may not be placed on the market, put into service for used for certain practices.[2]
- **High-risk AI systems:** these AI systems must satisfy a number of requirements to mitigate the risks before they may be placed on the market or used.[3]

Other requirements will also apply to AI models and AI systems capable of performing certain tasks:

- **General purpose AI models and systems**: these models and systems will be subject to specific information requirements. In certain cases, other requirements must be complied with in order to mitigate risks.[4]
- **Generative AI and chatbots**: these applications will be subject to specific transparency requirements depending on whether the system is or is not a high-risk system.[5]

The same AI system can sometimes be covered by multiple categories. A chatbot, for example, can be deployed for a high-risk application and/or based on a general purpose AI model. AI systems not covered by any of the categories described above are not required to comply with the requirements from the AI Act. Nevertheless, you must remember that AI systems and the development of AI systems may also be required to comply with requirements from other regulations such as the General Data Protection Regulation (GDPR).

To determine whether you are required to comply with requirements from the AI Act, it is important to first identify the category that covers your AI system. Below we discuss the different risk categories in more detail.

1.1. Prohibited AI systems

Certain AI practices bring about an unacceptable risk for people and society. These practices have therefore been prohibited since February 2025. This means that these systems may not be placed on the market, put into service or used for these practices. These prohibitions apply both to providers and deployers since 2 February 2025 (further explanation is provided under Step 3. Are we the provider or deployer of the AI system? on page 12).

[2] Chapter II, Article 5 AI Act.
[3] Chapter III, Article 6 through to 49 AI Act.
[4] Chapter V, Article 51 through to 56 AI Act.
[5] Chapter IV, Article 50 AI Act. Specific transparency requirements will also apply for emotion recognition and biometric categorisation systems. As these systems are also high-risk AI systems, they will also have to adhere to the requirement for these systems, as described in step 4.2.

Prohibited AI systems[6]

1. Systems intended to **manipulate human behaviour** with a view to restricting the free choice of individuals and which can result in significant harm to those persons.
2. Systems which **exploit the vulnerabilities** of persons due to their age, disability or a specific social or economic situation and which are likely to cause significant harm to those persons.
3. Systems that draw up a point system of rewards and punishments based on social behaviour or personality traits, known as **social scoring**, which could lead to detrimental or unfavourable treatment.
4. Prohibition on systems for making **risk assessments to predict the risk of a person committing a criminal offence**, based solely on profiling or personality or other traits.
5. Systems which create or expand **facial recognition databases** through the untargeted **scraping** of facial images from the internet or CCTV footage.
6. Systems for **emotion recognition** in the workplace and in education institutions, except where intended for medical or safety reasons.
7. Systems used for categorising **individual persons using biometric categorisation systems** in certain sensitive categories such as race and sexual orientation.
8. **The use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement.** There are a number of exceptions in cases in which use is strictly necessary, for example when searching for specific victims of obduction, trafficking in human beings or missing persons. These applications are subject to additional guarantees.

1.2. High-risk AI systems

High-risk AI systems may result in risks to health, safety or fundamental rights of natural persons, such as the right to privacy and the right not to be discriminated. At the same time, these systems can also have positive impact on natural persons and organisations, if they are reliable and the risks are mitigated. Against that background, from August 2026 onwards, high-risk AI systems must comply with a variety of requirements before being placed on the market, used or put into service. This means that during the development of the system, **providers** must ensure that the system satisfies these requirements before it is first placed on the market or used. A professional party that uses the AI system subject to its personal responsibility is considered a **deployer** (explained in more detail under Step 3. Are we the provider or deployer of the AI system? on page 12).

Deployers are also subject to obligations with the aim of mitigating risks resulting from the specific use of the system. There are two types of high-risk AI systems:

- **High-risk products**: AI systems that are directly or indirectly also subject to a selection of **existing product regulations** (see below). For example an AI system as a safety component of a lift or an AI system that in and of itself is a medical device.
- **High-risk applications**: AI systems developed and deployed for specific applications in 'high-risk application areas'. These are eight application areas for AI that range from AI for law enforcement to AI in education. Within those eight areas, around 30 different specific applications have been identified that result in high risks, such as AI systems that support the deployment of emergency first response services.

The product groups and application areas in which AI systems are categorised as high-risk appear in the figures below.

The obligations for this category also apply to high-risk products as from 2 August 2027 and to high-risk application areas as from 2 August 2026. The obligations are described under 4.2. High-risk AI on page 13.

[6] Article 5 AI Act, see also Commission Guidelines on prohibited artificial intelligence practices.

High-risk AI as (safety element of) existing products
These are products already regulated within the EU. A product is considered as representing a risk if in accordance with existing product regulations, third-party approval is required before the product can be placed on the market (conformity assessment). If AI is a safety-related component of the risk product or if the risk product itself is an AI system, it is considered as high-risk AI. This applies to products covered by the following product legislation:[7]

- **Machines** (Directive 2006/42/EC)
- **Toys** (Directive 2009/48/EC)
- **Recreational craft** (Directive 2013/53/EU)
- **Lifts** (Directive 2014/33/EU)
- **Equipment and protective systems intended for use in potentially explosive atmospheres** (Directive 2014/34/EU)
- **Radio equipment** (Directive 2014/53/EU)
- **Pressure equipment** (Directive 2014/68/EU)
- **Cableway installations** (Regulation (EU) 2016/424)
- **Personal protective equipment** (Regulation (EU) 2016/425)
- **Appliances burning gaseous fuels** (Regulation (EU) 2016/425)
- **Medical devices** (Regulation (EU) 2017/745)
- **In-vitro diagnostic medical devices** (Regulation (EU) 2017/746)

In addition, the AI Act contains a further list of products also considered as high-risk AI, but which are not subject to any direct requirements under the AI Act. Nevertheless, at a later moment, the requirements from the AI Act will be used to clarify the specific product legislation applicable to these products. It is not yet known when this will take place, and it will differ from product to product. The products in question are subject to the following product legislation:[8]

- **Civil aviation security** (Regulation (EC) 300/2008 and Regulation (EU) 2018/1139)
- **Two or three-wheeled vehicles and quadricycles** (Regulation (EU) 168/2013)
- **Agricultural and forestry vehicles** (Regulation (EU) 167/2013)
- **Marine equipment** (Directive 2014/90/EU)
- **Interoperability of the railway system in the EU** (Directive (EU) 2016/797)
- **Motor vehicles and trailers** (Regulation (EU) 2018/858 and Regulation (EU) 2019/2144)

High-risk application areas
An AI system is within the scope of one of the high-risk application areas if the provider intended the use of the AI system in one of these areas. In the documentation of the AI system, the provider must explicitly state the purpose, including the instructions for use, advertising materials and any other technical documentation. **Note:** Even if the provider did not intend the AI system as being high-risk when it was placed on the market, it may still be that in practice, a deployer does use the system for one of the high-risk application areas. In that case, the deployer is seen as the provider, and as such becomes responsible for the requirements imposed on high-risk AI systems. See also chapter 4.2.

There are eight high-risk application areas. This does not mean that all AI systems covered by the often abstractly described application areas are necessarily high-risk. A number of specific applications are listed for each area.[9]

Tip: First check whether your AI system is covered by one of the eight application areas and then determine whether your AI system is one of the AI systems described in that category. Only in that case are you dealing with a high-risk AI system that must comply with the requirements.

[7] Article 6(1) and Annex I, Section A AI Act.
[8] Article 2(2) and Annex I, Section B AI Act.
[9] Annex III AI Act.

1. **Biometrics**

- Remote biometric identification systems, unless the system is only used for verification.
- Systems used for biometric categorisation according to sensitive or protected attributes.
- Systems for emotion recognition.

2. **Critical infrastructure**

- Systems intended to be used as safety components for the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity.

3. **Education and vocational training**

- Systems for admission to or allocation of (vocational) education.
- Systems for evaluating learning outcomes.
- Systems for assessing the level of (vocational) education.
- Systems for monitoring students during tests.

4. **Employment, workers' management and access to self employment.**

- Systems for the recruitment or selection of candidates.
- Systems to be used to make decisions affecting terms of work-related relationships, the allocation of tasks or the monitoring and evaluation of workers.

5. **Essential private services and public services and benefits**

- Systems for evaluating the eligibility to essential public assistance benefits and services.
- Systems for evaluating the creditworthiness or credit score of natural persons unless used for the purposes of detecting financial fraud.
- Systems for risk assessment and pricing in relation to life and health insurance.
- Systems for evaluating emergency calls and prioritising the dispatch of emergency first response services and emergency health care patient triage systems.

6. **Law enforcement**

- Systems for law enforcement to assess the risk of a natural person becoming the victim of criminal offences.
- Systems for law enforcement to be deployed as polygraphs or similar tools.
- Systems for law enforcement for evaluating the reliability of evidence.
- Systems for law enforcement for assessing or predicting the risk of a natural personal offending or to assess past criminal behaviour of natural persons or groups.
- Systems for law enforcement for the profiling of natural persons in the course of detection, investigation or prosecution of criminal offences.

7. **Migration, asylum and border control**

- Systems for public authorities to be used as polygraphs or similar tools.
- Systems for public authorities for assessing a security risk, the risk of irregular migration or a health risk upon entry into a country.
- Systems for public authorities to assist in the examination of applications for asylum, visa or residence permit, including associated complaints.
- Systems for public authorities for detecting, recognising or identifying natural persons, with the exception of the verification of travel documents.

8. **Administration of justice and democratic processes**

- Systems to be used by a judicial authority to assist in applying the law and resolving disputes and researching and interpreting facts and applying the law to a concrete set of facts.
- Systems for influencing the outcome of an election or referendum or the voting behaviour of natural persons, with the exception of tools used to support political campaigns from an administrative or logistic point of view.

Exceptions to high-risk application areas

There are a number of specific exceptions in which AI systems are covered by one of the application areas but which are not seen as high-risk AI. This applies where there is no significant risk to health, safety or fundamental human rights. This for example applies if an AI system has **no significant impact on the outcome of a decision,** for example because the system is intended for**:**[10]

- Performing a narrow procedural task;
- Improving the result of a previously completed human activity;
- Detecting decision-making patterns or deviations from prior decision-making patterns and not meant to replace or influence the previously completed human assessment;
- Performing a preparatory task to an assessment relevant to one of the high-risk application areas.

It should also be noted that an AI system used for profiling natural persons cannot make use of this exception. If you have determined that your (non-profiling) AI system is subject to one of the exceptions, you must record this fact and register the AI system in the EU database for high-risk AI systems.[11] At a later moment, the European Commission will draw up a list of examples to clarify what is and what is not covered by the exceptions.

1.3. General purpose AI models and AI systems

An AI model is an essential component of an AI system, but is not an AI system in and of itself. This requires more elements, for example a user interface.[12]

A **general purpose AI model** (General Purpose AI) can successfully perform a wide range of different tasks and as such can be integrated in a variety of AI systems. These models are often trained on large volumes of data using self-supervision techniques.[13]

The broad deployability of these models via specific AI systems means that they are used for a wide range of applications. These can include high-risk applications. Due to the potential large impact of these models, from August 2025 onwards, they must comply with various requirements.

If an AI system is based on a general purpose AI model which itself can actually serve multiple purposes, then it is a **general purpose AI system.**[14]

The obligations applicable to this category apply from 2 August 2025 and are described under 4.3. General purpose AI models and systems on page 18.

[10] Article 6(3) AI Act.
[11] Article 6(4) AI Act.
[12] Consideration 97 AI Act.
[13] Article 3(63) AI Act.
[14] Article 3(66) AI Act.

1.4. Generative AI and Chatbots

Certain AI systems are subject to transparency obligations.[15] These are systems with which natural persons often interact directly. It must therefore be clear to these natural persons that they are interacting with AI or that the content has been manipulated or generated.

- Systems used for generating audio, images, video or text (**generative AI**);
- Systems made for interaction (**chatbots**).

The obligations applicable to this category apply from 2 August 2026 and are described under 4.4. Generative AI and Chatbots on page 19.

1.5. Other AI

See 4.5. Other AI on page 20 for more information on AI systems not covered by one of the risk categories described above.

[15] Article 50 AI Act.

Step 2. Is our system 'AI' classified according to the AI Act?

The AI Act imposes regulations on AI systems. There are different ideas about what AI is and what is not AI. The AI Act offers the following definition, which is intended to demarcate the nature of AI as a product on the market:

"An AI system means 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****."*[16]

These different elements can be present both in the development phase and in the use phase. What is the meaning of the terms used in this definition?[17]

- **Autonomy**: This element is satisfied if autonomy is present in a system to a certain extent, even if very limited. Systems without any form of autonomy are systems that only operate if human actions or interventions are required for all actions by that system.
- **Adaptiveness:** It is stated that a system 'may' exhibit adaptiveness after deployment. Although adaptiveness is therefore not identified as a decisive element, its presence is an indication that the system is an AI system.
- **It infers how to generate output on the basis of input (capacity to infer):** This relates not only to generating output during the 'use phase' but also the capacity of an AI system to infer models and/or algorithms from data during the development phase.

What does this cover?[18]

- Systems that make use of **machine learning** in which the system learns how certain objectives can be achieved on the basis of data. Examples of machine learning are (un)supervised learning, self-supervised learning, reinforcement learning and deep learning.
- Systems that make use of **knowledge and logic-based approaches** which make learning, reasoning or modelling possible on the basis of determined knowledge or a symbolic representation of a task to be solved. Examples of these approaches are knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning, expert systems and search and optimisation methods.

What is **not** covered?

- Systems based on rules laid down exclusively by natural persons to conduct automatic actions. Some of these systems can to a certain extent derive how to generate output from input received, but are still beyond the definition because they are only able to analyse patterns to a limited extent or are unable to autonomously adapt their output. Examples can be systems for improved mathematical optimisation, standard data processing, systems based on classic heuristics and simple prediction systems.
- Systems designed to be used with full human intervention. These systems do not operate with a minimum level of autonomy.

[16] Article 3(1) AI Act.

[17] Commission Guidelines on the definition of an artificial intelligence system.

[18] Consideration 12 AI Act.

The European Commission has issued a guideline to further clarify the definition of AI. You can find the latest version on this guideline at ondernemersplein.nl.

If your system is not considered AI under the AI Act but is covered by one of the risk categories, it is important to hold a discussion within your organisation about the extent to which the system still represents risks and to mitigate these risks by complying with (specific) requirements from the AI Act. Systems beyond the scope of the AI Act may nevertheless still have to comply with requirements from other legislation and regulations.

Step 3. Are we the provider or deployer of the AI system?

Once you have determined the risk category that covers you AI system and whether your AI system is in fact subject to the AI Act, you must then determine whether you are the provider or deployer.

- **Provider**: a person or organisation that develops or commissions the development of an AI system or model and places it on the market or puts the AI system into service.[19]
- **Deployer**: a person or organisation using an AI system under its personal authority. This does not include non-professional use.[20]

The description of the requirements in step 4 describes for each risk category which obligations apply to providers and deployers. Each is required to comply with other obligations. The strictest obligations apply to providers.

Note: As deployer, in certain cases you can also become provider of a high-risk AI system such that you are required to comply with the high-risk obligations for providers.[21] This is further explained in steps 4.2. High-risk AI on page 13 and 4.3. General purpose AI models and systems on page 18.

Note: the AI Act also includes other roles such as authorised representative, importer and distributor.[22] The obligations governing these actors are not discussed in this guide.

[19] Article 3(3) AI Act.

[20] Article 3(4) AI Act.

[21] Article 25 AI Act.

[22] Article 3(5), (6) and (7), Articles 22, 23 and 24.

Step 4. What obligations must we comply with?

4.1. Prohibited AI practices

These AI practices result in unacceptable risk and have therefore been prohibited since 2 February 2025. This means that AI systems cannot be placed on the market or used for these practices. These prohibitions apply to both **providers** and **deployers.**[23]

There are sharply demarcated exceptions to the prohibition on the use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, and the use of those systems must be provided with a basis in national legislation. There are also additional guarantees relating to the deployment of these systems.

4.2. High-risk AI

The majority of requirements from the AI Act will apply to high-risk AI systems. **Providers** must comply with various obligations such as:[24]

- System for risk management;
- Data and data governance;
- Technical documentation;
- Record-keeping (logs);
- Transparency and information;
- Human oversight;
- Accuracy, robustness and cybersecurity;
- Quality management system;
- Monitoring.

If you as provider comply or believe you comply with all these obligations, you will be required to conduct a **conformity assessment**. In certain cases you can conduct this assessment yourself, while in other cases it must be conducted by a third party on your behalf.[25] A future version of this guide will explain in more detail when you are required to conduct which procedure.

Deployers must also comply with various obligations. Additional obligations apply to government organisations using AI systems.[26]

Each obligation is explained in the figure below. These obligations will be further elaborated over the coming years in European standards. Participation will be organised via the standardisation institutes of the European Member States. In the Netherlands this is the NEN[27].

Note: In two cases, as deployer of a high-risk AI system, you yourself can become the provider of that system:[28]

- When you as deployer place your own name or trademark on the high-risk system;
- When you as deployer make a substantial modification to the high-risk AI system that was not intended by the provider as a consequence of which the system no longer complies with the requirements or as a consequence of which the purpose of the system intended by the provider changes. This latter situation arises if you make use of an AI system that was not intended for high-risk applications, for any such applications.

[23] Article 5 AI Act.
[24] Article 16 and Section 2 of Chapter III (Articles 8-15) AI Act.
[25] Article 43 AI Act.
[26] Articles 26 and 27 AI Act.
[27] https://www.nen.nl/ict/digitale-ethiek-en-veiligheid/ai.
[28] Article 25 AI Act.

Requirements for high-risk AI systems

1. System for risk management[29]

Various steps must be taken for this system:

- Identification and analysis of foreseeable risks the system can pose to health, safety or fundamental rights.
- Taking suitable risk management measures to ensure that the risks that remain following implementation of these measures are acceptable.

The following points must be taken into account:

- The risks must be identified and dealt with before the AI system is placed on the market or used and subsequently continuously during the use of the AI system.
- Foreseeable abuse of the system must be taken into account.
- The context of the use, including the knowledge and experience of the deployer of such AI systems or the fact that children and vulnerable groups may experience consequences of the AI system, must be taken into account. It may for example be necessary to offer training to the people working with the AI system.
- The risk management measures must be tested to check that they are actually effective. This must be carried out on the basis of benchmarks appropriate to the purpose for which the AI system is deployed.
- If a risk management system must also be established pursuant to existing product legislation, this may be combined to form a single risk management system.

2. Data and data governance[30]

Different requirements are imposed on the datasets used for training, validating and testing high-risk AI systems.

- Data management appropriate to the purpose of the AI system, including:
  - The registration of the processes, including processes for data gathering and data processing;
  - The recording of assumptions about the datasets;
  - An assessment of the availability, quantity and suitability of the datasets including possible biases that could have consequences for natural persons;
  - Measures for tracing, preventing and mitigating biases;
  - Tackling shortcomings in the datasets that may prevent compliance with the AI Act (for example mitigating risks according to the risk management system).
- For the purpose for which they are used, datasets must be sufficiently representative and as far as possible error-free. The context in which the AI system is to be used must also be taken into account; for example the geographical or social context.
- Subject to a number of strict conditions, special categories of personal data (a term from the General Data Protection Regulation) may be processed as a means of tackling bias.

[29] Article 9 AI Act.
[30] Article 10 AI Act.

3. Technical documentation[31]

The technical documentation must demonstrate that the high-risk AI system complies with the requirements laid down in the AI Act. The technical documentation must among others include:

- A general description of the AI system including the intended purpose of the system, the name of the provider and instructions for use;
- A detailed description of the elements of the AI system and of the development process for that system, including the steps in development, the design choices, the expected output from the system, the risk management system and the datasets used;
- Detailed information about the monitoring, operation and control of the AI system, including the degree of accuracy at individual and general level, risks, the system for evaluation during use and measures for monitoring and human oversight;
- An overview of the applicable standards;
- The EU conformity declaration (the CE mark).

SME enterprises can record their technical documentation in a simplified manner. At a future moment, the European Commission will issue a relevant form.

4. Record-keeping (logs)[32]

Automatic logs must be retained during the lifecycle of the AI system so that risks can be traced in a timely manner and the operation of the system can be monitored.
These logs must be stored for at least six months. At least the following events must be recorded:

- The duration of each use of the AI system;
- The input data and the control of that data by the AI system (and the reference database);
- The identification of the natural persons involved in the verification of the results.

5. Transparency and information[33]

The provider of the AI system knows how the system operates and how it should be used. For that reason, the provider must ensure that the AI system is sufficiently transparent so that deployers understand how they can correctly make use of the output from the system.

With this in mind, **instructions for use** must be drawn up, that include at least the following points:

- Contact details;
- The purpose, characteristics, capacities and limitations of the performance of the AI system;
- The measures for human oversight.

6. Human oversight[34]

High-risk AI systems must be designed by the provider in such a way that during use they can be effectively overseen by natural persons in order to mitigate the risks for natural persons. Human oversight shall be context dependent – the greater the risks, the stricter the oversight must be.
The measures for oversight may be technical in nature (for example a clear human-machine interface), or measures that must be undertaken by the deployer (for example a compulsory course for their personnel).

[31] Article 11 AI Act.

[32] Article 12 AI Act.

[33] Article 13 AI Act.

[34] Article 14 AI Act.

The eventual objective of these measures is to ensure that the natural persons who use the AI system are capable of the following:

- They understand the capacities of the system and can monitor its functioning;
- They are aware of automation bias;
- They can correctly interpret and if necessary ignore or replace the output;
- They can halt the system.

7. Accuracy, robustness and cybersecurity[35]

High-risk AI systems must offer an appropriate level of accuracy, robustness and cybersecurity. To achieve this, benchmarks and measuring methods are developed by the European Commission.

At least the following measures must be mentioned:

- Technical and organisational measures to prevent errors that occur in interaction between the AI system and natural persons;
- Solutions for robustness such as backups or security measures in the event of defects;
- Removing or mitigating negative influencing of the system by limiting feedback loops;
- Cybersecurity that prevents unauthorised third-party access by tracing, responding to and dealing with attacks. These are attacks aimed at data poisoning, model poisoning, adapting input or obtaining confidential data.

8. Quality management system[36]

The quality management system must ensure that the requirements from the AI Act are complied with. How extensive the quality management system must be will depend on the size of the organisation. For example by documenting the following:

- A strategy for compliance;
- Techniques, procedures and measures for the design, development and quality assurance of the AI system;
- Whether standardisation is used;
- Systems and procedures for data management, risk management, monitoring, incident reporting and documentation.

9. Monitoring[37]

As soon as an AI system has been placed on the market or is in use, providers must monitor the system on the basis of use data, thereby determining whether the system continues to comply with the requirements from the AI Act. For this purpose, providers must draw up a monitoring plan.

If the provider of a high-risk AI system discovers that the system no longer functions in compliance with the AI Act, corrective measures must be taken immediately to correct the situation. This may even include recalling the system if necessary. The provider must also work alongside the deployer and duly inform the surveillance authorities.

Serious incidents involving the AI system must be reported to the surveillance authorities.[38]

[35] Article 15 AI Act.
[36] Article 17 AI Act.
[37] Article 72 AI Act.
[38] Article 73 AI Act.

Other requirements

- The registration of the high-risk AI system in the EU database.[39]
- The contact details of the provider must be registered with the AI system.[40]
- The technical documentation, documentation concerning the quality management system and documentation concerning the conformity assessment must be kept for 10 years.[41]

Obligations for deployers of high-risk AI systems
Not only providers but also the deployers of high-risk AI systems are subject to obligations. After all they are the parties who control how the AI system is used in practice and as such have a major impact on the risks that can occur.

Deployers must:[42]

- Take appropriate technical and organisational measures to ensure that the high-risk AI system is used in accordance with the instructions for use;
- Assign human oversight to natural persons who have the necessary competence, training and authority;
- Ensure that the input data is relevant and sufficiently representative, wherever possible;
- Monitor the operation of the AI system on the basis of the instructions for use;
- If the deployer has reason to believe that the system no longer complies with the requirements from the AI Act, the deployer must duly inform the provider and cease use of the system;
- Inform the provider and surveillance authorities of possible risks and serious incidents that have occurred;
- Keep the logbook under their control for at least six months;
- Inform worker representation if the AI system is to be deployed on the shop floor;
- Duly inform people if decisions are taken about natural persons using the high-risk AI system;
- If use is made of AI for emotion recognition or biometric categorisation, the natural persons in respect of whom the system is used must be duly informed.

Specific obligations for government organisations as deployers In addition to the obligations described above, government organisations must comply with a number of additional obligations:

- Register use of a high-risk system in the EU database;[43]
- Assess the potential consequences for fundamental rights if the high-risk AI system is used with a view to the specific context within which use takes place (a **fundamental rights impact assessment**). They will for example consider the duration of use, the processes within which the system is used and the potential impact of use on the fundamental rights of natural persons and groups. Following identification of the risks, deployers must take measures for human oversight and deal with possible risks. A report must also be submitted to the market surveillance authorities unless an appeal can be made to an exception based on public safety or protection of human health.[44]

Note: This obligation also applies to private entities providing public services, the use of AI systems for assessing the creditworthiness of natural persons and AI systems for risk assessments for life and health insurance.

[39] Article 49 AI Act.
[40] Article 16(b) AI Act.
[41] Article 18 AI Act.
[42] Article 26 AI Act.
[43] Article 49(3) AI Act.
[44] Article 27 AI Act.

4.3. General purpose AI models and systems

Obligations for providers of general purpose AI models[45]
General purpose AI models can be integrated in all kinds of different AI systems. It is essential that the providers of these AI systems know what the AI model is and is not capable of. Specific requirements are also imposed on the training of these models because training often makes use of large datasets. The providers of these models must:

- Draw up technical documentation of the model including the training and testing process and the results and evaluation;
- Draw up and keep up to date information and documentation for providers of AI systems who intend to integrate the model in their AI system. The information must provide a good understanding of the capacities and limitations of the AI model and must enable the provider of the AI system to comply with the obligations from the AI Act.
- Draw up a policy to ensure that they train the model without infringing the copyrights of natural persons and organisations;
- Draw up and publish a sufficiently detailed summary about the content used for training the AI model.

Providers of open source models are not required to comply with the first two obligations (technical documentation and drawing up information for downstream providers).

Obligations for providers of general purpose AI models with systemic risks[46]
In certain cases, general purpose AI models can generate systemic risks. This applies if the model has high impact capacity, for example due to the scope of the model or due to (potential) negative impact on public health, safety, fundamental rights or society as a whole. This is at least assumed if at least 10^{25} floating point operations (FLOPs) are used to train the model. On the basis of specific criteria, the European Commission can also determine that the model has a similar major impact in some other way. These models must:

- Comply with the obligations for general purpose AI models;
- Implement model evaluations to map out the systemic risks;
- Mitigate systemic risks;
- Record information about serious incidents and report those incidents to the AI Office;
- Ensure appropriate cybersecurity.

Note: these obligations only apply to the largest AI models.
Providers of these models with systemic risks cannot appeal to an exception for open source.

[45] Article 53 AI Act.
[46] Article 55 AI Act.

What rights do you have if you integrate a general purpose AI model in your (high-risk) AI system?
As indicated above, you must at least receive information and documentation to enable you to determine for yourself how you can make use of the model in your AI system for the chosen purpose. If you include the model in a high-risk AI system, as a provider you must then still comply with the obligations from the AI Act.

How should you deal with general purpose AI systems? As indicated in 1.3. General purpose AI models and AI systems on page 8, there are also AI systems that can serve multiple purposes. Take for example the widely known AI chatbots. **Note:** If you deploy these systems for high-risk purposes, according to the AI Act you yourself become a provider of a high-risk AI system.[47] It is then up to you to comply with the applicable obligations. In this situation it is very difficult to comply with the obligations for a high-risk AI system, which means that you may run the risk of receiving a penalty.

4.4. Generative AI and Chatbots

To ensure that natural persons know whether they are talking to an AI system or are seeing content generated by AI, transparency obligations are imposed on generative AI and chatbots.

Rules for providers of chatbots[48]
Providers of systems designed for direct interaction with natural persons must ensure that these natural persons are informed that they are interacting with an AI system.

Rules for providers of generative AI[49]
Providers of systems that generate audio, image, video or text content must ensure that the output is marked in a machine readable format so that the output can be detected as artificially generated or manipulated.

Rules for deployers of generative AI[50]
Deployers of systems that generate audio, image or video content must ensure that it is clear that the content is artificially generated or manipulated. This can for example be achieved by applying a watermark. For creative, satirical, fictional or analogue work, this may be carried out in a way that does not ruin the work.

A special regime applies to artificially generated text. Only in cases where texts are used with the purpose of ‘informing the public on matters of public interest’, the fact must be disclosed that the text has been artificially generated or manipulated. If there is editorial review and responsibility, this need not be carried out.

Rules for deployers of emotion recognition systems or systems for biometric categorisation[51]
The deployers of these AI systems must inform the natural persons exposed to these systems about how the system works.

[47] Article 25(1)(c) AI Act.
[48] Article 50(1) AI Act.
[49] Article 50(2) AI Act.
[50] Article 50(4) AI Act.
[51] Article 50(3) AI Act.

4.5. Other AI

AI systems beyond the categories referred to above are not required to comply with requirements according to the AI Act.

But note: if you as **deployer** make use of 'other category' AI systems for a high-risk application as referred to in the AI Act (see 1.2. High-risk AI systems on page 5), it automatically becomes a high-risk AI system and you must comply with the requirements from the AI Act as a system **provider**.[52]

[52] Article 25(1)(c) AI Act.

Colofon

Dit is een uitgave van;

Ministerie van Economische Zaken
Postbus 20901 | 2500 EX Den Haag

www.rijksoverheid.nl