akd
benelux law firm

Whitepaper AI Act

Requirements and obligations to prepare for the AI Act

Introduction to the AI Act

- The AI Act aims to provide AI developers ('providers') and deployers with clear requirements and obligations regarding specific uses of AI.

- The AI Act will enter into force 20 days after its publication in the Official Journal (July 12, 2024), and **will be fully applicable 2 years later (2 August 2026)**, with some exceptions: prohibitions will take effect after six months, the governance rules and the obligations for general-purpose AI models become applicable after 12 months and the rules for AI systems - embedded into regulated products - will apply after 36 months.

About this whitepaper

- This whitepaper provides an overview of (a selection of) relevant clauses and the requirements and obligations following from these clauses. It serves to help you or your organisation to prepare for the AI Act. Where relevant, references to the applicable recitals and articles have been included at the bottom of the page.

- The information in this whitepaper is based on general assumptions only and thus not based on specific cases or circumstances, unless this is explicitly mentioned.

- Feel free to contact AKD if you have questions or other requests. Relevant contact information is included on the contact page.

- More information about AKD? Go to www.akd.eu.

- More information about the AI Act? Go to EU Commission.

Content

Definition and scope

General requirements

High-risk systems

Provider obligations

Deployer obligations

General-purpose AI

Link with GDPR

Main take-aways

Definition and scope

Definition of AI

The AI Act aims to provide requirements and obligations regarding the use of AI. This is to ensure trustworthy AI, without unnecessarily hindering innovation and technological developments. In order to understand whether you or your organisation is bound by the AI Act, one should start with the definition of "AI" or "AI system":

> *"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."*

A key characteristic of AI systems is their capability to infer. This refers to:

- the process of obtaining the outputs, such as predictions, content, recommendations, or decisions, which can influence physical and virtual environments
- a capability of AI systems to derive models or algorithms, or both, from inputs or data techniques that enable inference while building an AI system, such as machine learning approaches

The AI Act does not apply to simpler traditional software systems or programming approaches. Neither does it cover systems that are based on the rules defined solely by natural persons to automatically execute operations.

Click here for examples.

Recitals 12-13 AI Act
Articles 3 (1), (3), (4), (6) and (7) AI Act

Applicable to whom?

Providers

Provider: a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Deployers

Deployer: a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Importers and distributors

Importer: a natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

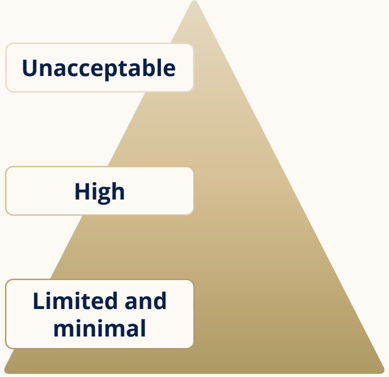
Distributor: a natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

The AI Act may also apply to parties outside the EU (click)!

The AI Act consists of a risk-based approach. This means that more (or stricter) requirements apply to AI systems with high(er) risks. The risk of an AI system is determined on the basis of the combination of the probability of an occurrence of harm and the severity of that harm. It is thus relevant to carry out a risk assessment prior to using an AI system or to putting one on the market.

Due to their risk level, some practices are forbidden ('unacceptable risk'). These practices relate to being contradictory to values of respect for human dignity, freedom, equality, democracy and the rule of law and fundamental rights.

An example of a forbidden practice is the creation of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.



Fines

Non-compliance with the prohibition of the AI practices referred to in Article 5 shall be subject to administrative fines of up to 35,000,000 EUR or, if the offender is an undertaking, up to 7% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Other violations: subject to administrative fines of up to 15,000,000 EUR or, if the offender is an undertaking, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher or administrative fines of up to 7,500,000 EUR or, if the offender is an undertaking, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher.

Article 5 AI Act

General requirements

AI literacy

Regardless of the risk level of the AI system, both the provider and the deployer must make sure that their employees and any other person dealing with their AI system(s) on behalf of the provider have a sufficient level of "AI literacy".

AI literacy means: "skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of the AI Act, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause".

Providers and deployers must, by means of AI literacy:

- Be able to make informed decisions about AI systems.
- Equip their employees or others with relevant notions, such as understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI will have an impact on them.
- Provide all relevant actors with the insights of the AI Act to ensure the appropriate compliance.

Article 4 AI Act

Transparency

Several requirements regarding transparency apply to both the provider and the deployer. These requirements apply regardless of the risk level of the AI system.

Providers

- AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious.
- As to AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated by the provider.

Deployers

- Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with the GDPR.
- Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work.

High-risk systems

High risk?

To determine whether the AI system falls within the high-risk category, the following steps should be taken:

Step 1

Determine the goal and objective of the AI system.

The objectives of the AI system may be different from the intended purpose of the AI system in a specific context. Environments should be understood to be the contexts in which the AI systems operate, whereas outputs generated by the AI system reflect different functions performed by AI systems and include predictions, content, recommendations or decisions.

Step 2

Assess whether the AI system is covered by legislation included in Annex I of the AI Act and, pursuant to such legislation, a third-party conformity assessment is required. If so, the AI system is high risk.

As regards AI systems that are safety components of products, or which are themselves products, falling within the scope of certain EU harmonisation legislation listed in an annex to the AI Act, it is appropriate to classify them as high-risk under the AI Act if the product concerned undergoes the conformity assessment procedure with a third-party conformity assessment body. Examples are: machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, in vitro diagnostic medical devices, automotive and aviation.

Recitals 47-53 AI Act
Article 6 AI Act

Step 3

Assess whether the AI system is covered by the systems as included in Annex III of the AI Act. If so, the AI system is high risk.

Step 4

Assess whether the derogation of Article 6(3) AI Act can be invoked if there are no risks to health, safety or fundamental rights:

- the AI system is intended to perform a narrow procedural task, such as an AI system that transforms unstructured data into structured data, an AI system that classifies incoming documents into categories or an AI system that is used to detect duplicates among a large number of applications
- the AI system is intended to improve the result of a previously completed human activity; the AI system provides only an additional layer to a human activity with consequently lowered risk, such as AI systems that are intended to improve the language used in previously drafted documents, for example in relation to professional tone, academic style of language or by aligning text to a certain brand messaging
- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review, for instance AI systems that, given a certain grading pattern of a teacher, can be used to check ex post whether the teacher may have deviated from the grading pattern so as to flag potential inconsistencies or anomalies
- the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III. This includes various functions from indexing, searching, text and speech processing or linking data to other data sources, or AI systems used for translation of initial documents.

Derogation applies? No high-risk AI system!

Requirements for high-risk systems

High-risk AI systems should only be placed on the market, put into service or used if they comply with certain mandatory requirements. Those requirements should ensure that high-risk AI systems do not pose unacceptable risks. It is generally up to the provider to meet these requirements. Some of the relevant requirements are:

Risk management system

- A continuous process that runs throughout the entire lifecycle of the AI system
- Systematic review and updating is required
- Identification and analysis of known and foreseeable risks, in accordance with the intended purpose of use
- Adoption of appropriate risk management measures

Technical documentation

- Technical documentation must demonstrate compliance with relevant requirements
- Documentation must include, for example, a general description of the AI system and a detailed description of elements of the AI system and the development process
- Less strict requirements for SMEs and start-ups

Record-keeping

- The AI system must be able to automatically record events (logging)
- Logging must enable the identification of possible high-risk situations
- Logging requirements depend on the applicable high-risk qualification (Annex I or Annex III)

Human oversight

- The AI system must be developed in a way that allows for human oversight
- Human oversight shall aim to prevent possible risks from emerging
- Specific requirements for providers with regard to deployers

Accuracy

- The AI system must be developed in a way that an appropriate level of accuracy can be reached
- The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use
- The EU Commission is to provide EU benchmarks

Cyber security

- High-risk AI systems shall be as resilient as possible
- The technical solutions aiming to ensure the cybersecurity of high-risk AI systems shall be appropriate to the relevant circumstances and the risks
- The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control data poisoning or model poisoning, adversarial examples or model evasion, confidentiality attacks or model flaws

Recitals 64-77 AI Act
Articles 8-15 AI Act

Obligations of the provider

In addition to making sure the high-risk AI system meets the relevant requirements, it must also adhere to several obligations when placing high-risk systems on the market. This is the responsibility of the provider. The following obligations apply:

- Include contact information on the AI system
- Have in place a quality management system
- Have in place documentation
- Keep and store generated logs
- Carry out a conformity assessment and draw up a declaration of conformity
- Affix the CE-marking on the AI system
- Appoint a representative

Several of these obligations are explained below.

Quality management system

A quality management system should help the provider to comply with the AI Act. The system must at least include the following aspects:

- A strategy for compliance: how to become compliant, how to remain compliant?
- Techniques, procedures and systematic actions to be used for the design, design control and design verification of the high-risk AI system and for the development, quality control and quality assurance of the high-risk AI system;
- When and how tests and validation processes are carried out;
- Systems and procedures for data management;
- A post-market monitoring system;
- Incident reporting procedures;
- An accountability framework setting out the responsibilities of the management and other staff.

Conformity assessment

In order to ensure a high level of trustworthiness of high-risk AI systems, the systems should be subject to a conformity assessment prior to being placed on the market. Depending on the type of high-risk AI system, the provider may either carry out the conformity assessment himself or shall engage a notified body.

Exceptions:

- High-risk systems that are covered by legislation as listed in Annex I Section A shall be assessed as described in applicable relevant legislation instead;
- If authorised by a market surveillance authority.

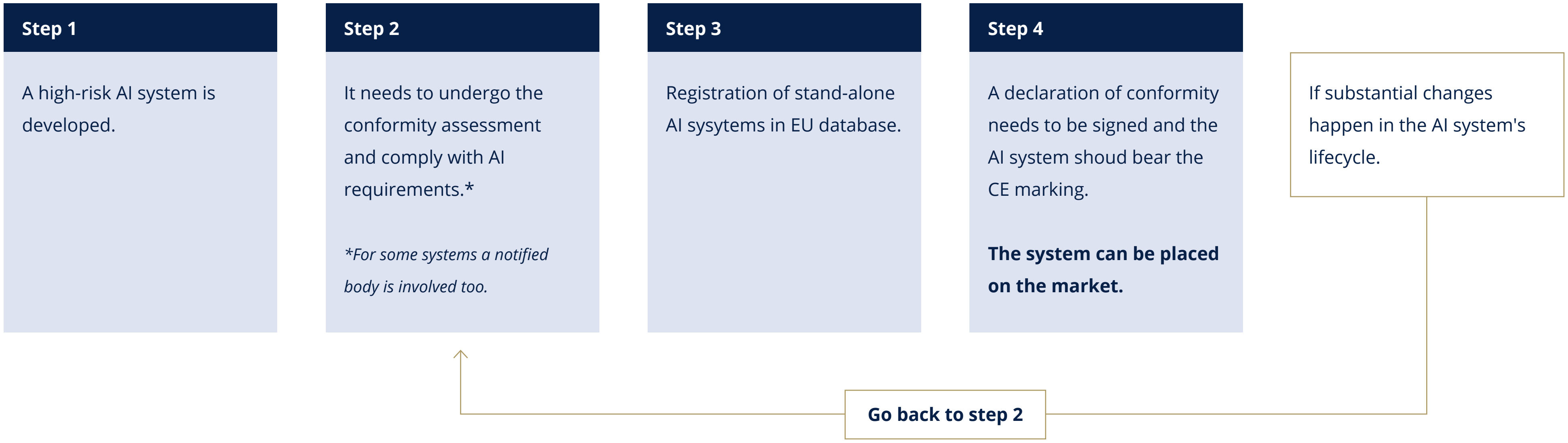
The conformity assessment must be carried out again in case of substantial modification. Changes occurring to the algorithm and the performance of AI systems which continue to 'learn' after being placed on the market or put into service, namely automatically adapting how functions are carried out, should not constitute a substantial modification, provided that those changes have been pre-determined by the provider and assessed at the moment of the conformity assessment.

If the conformity assessment has been carried out and the results are positive, the provider must draw up a so-called declaration of conformity. The declaration must be kept for a period of ten (10) years after being placed on the market and must be provided to relevant authorities if requested.

In addition, a CE-marking must be applied to show that the AI system has passed the conformity assessment. For high-risk AI systems embedded in a product, a physical CE marking should be affixed, and may be complemented by a digital CE marking. For high-risk AI systems only provided digitally, a digital CE marking should be used.

Recitals 79, 123-130 AI Act
Articles 16-22 AI Act
Articles 34-48 AI Act

Steps to take for the provider of a high-risk AI system



Step 1

A high-risk AI system is developed.

Step 2

It needs to undergo the conformity assessment and comply with AI requirements.*

**For some systems a notified body is involved too.*

Step 3

Registration of stand-alone AI sysytems in EU database.

Step 4

A declaration of conformity needs to be signed and the AI system shoud bear the CE marking.

The system can be placed on the market.

If substantial changes happen in the AI system's lifecycle.

Go back to step 2

Obligations of the deployer

General obligations

Given the nature of AI systems and the risks to safety and fundamental rights possibly associated with their use, including as regards the need to ensure proper monitoring of the performance of a high-risk AI system in a real-life setting, it is appropriate to set specific responsibilities for deployers. The following obligations are in place:

- Appropriate technical and organisational measures must be taken to ensure the AI system is used in accordance with the applicable instructions
- Human oversight must be assigned to persons who have the necessary competence, training and authority
- The input data must be relevant and sufficiently representative in view of the intended purpose of the AI system
- The AI system must be monitored on the basis of the instructions for use
- If deployers have reason to consider that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk, they shall, without undue delay, inform the provider or distributor and the relevant market surveillance authority, and shall suspend the use of that system
- If deployers have identified a serious incident, they shall also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident
- Deployers shall keep the logs automatically generated by that high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the high-risk AI system, of at least six months
- Deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system
- Deployers of high-risk AI systems that are public authorities, or EU institutions, bodies, offices or agencies shall comply with the registration obligations referred to in Article 49
- Deployers shall use information obtained from the provider in light of the AI system for purposes of carrying out a data protection impact assessment if needed under the GDPR

Fundamental rights impact assessment

In order to efficiently ensure that fundamental rights are protected, deployers of high-risk AI systems that are bodies governed by public law, or private entities providing public services and deployers of certain high-risk AI systems listed in an annex to the AI Act, such as banking or insurance entities, should carry out a fundamental rights impact assessment prior to putting it into use.

The assessment shall consist of:

1. A description of the deployer's processes in which the high-risk AI system will be used
2. A description of the period of time within which, and the frequency with which, each high-risk AI system is intended to be used;
3. The categories of natural persons and groups likely to be affected by its use in the specific context;
4. The specific risks of harm likely to have an impact on the categories of natural persons or groups of persons;
5. A description of the implementation of human oversight measures, according to the instructions for use;
6. The measures to be taken in the case of the materialisation of those risks, including the arrangements for internal governance and complaint mechanisms.

Recitals 91-95 AI Act
Article 12 AI Act

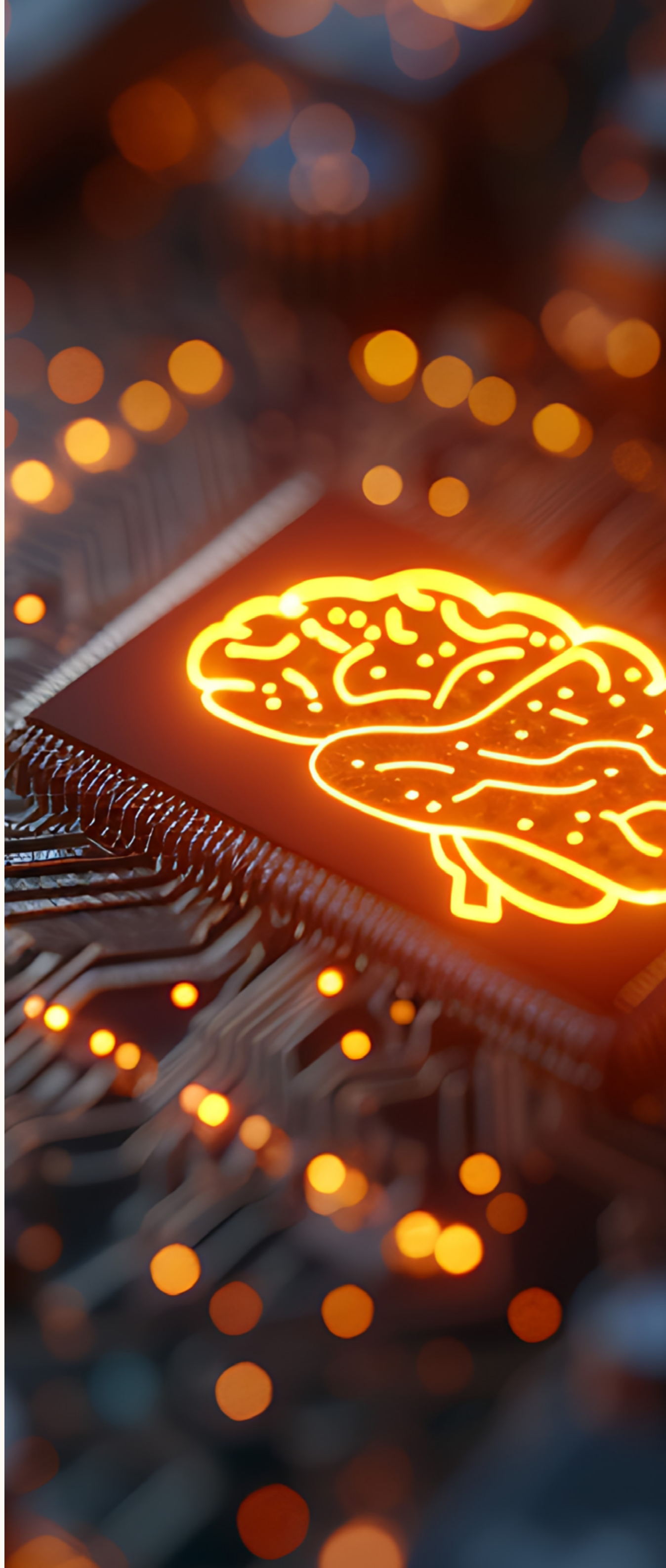
The assessment requirement applies to the first use of the relevant AI system for a specific purpose only. The deployer may, in similar cases, rely on previously conducted fundamental rights impact assessments or existing impact assessments carried out by provider. If all relevant requirements have already been assessed by means of a data protection impact assessment under the GDPR, the additional assessment under the AI Act is not required.

The assessment requirement is also applicable to:

- Educational bodies
- Healthcare providers
- Housing cooperations
- Social services providers
- Providers of legal or administrative services

Possible format: Impact Assessment for Algorithms (IAMA)

Recitals 96 AI Act
Article 27 AI Act



General-purpose AI

The AI Act contains specific rules regarding "general-purpose AI". A model (within the context of an algorithm) is classified as general-purpose AI if the following conditions are met. The model is an AI model:

- that displays significant generality; and
- that is capable of competently performing 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.

Exception: AI models that are used for research, development or prototyping activities before being placed on the market are not classified as general-purpose AI models.

Examples

The key functional characteristics of the AI model are relevant for determining whether a model is considered a general-purpose AI model. General-purpose AI models are typically trained on large amounts of data, through various methods, such as self-supervised, unsupervised or reinforcement learning.

Large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks.

Other examples:

ChatGPT DALL.E Gemini Midjourney

Recitals 97, 99, 110 and 111 AI Act
Articles 3 (63), 51 AI Act

Points of attention

It is important to note that:

- AI models do not constitute AI systems on their own – AI models require the addition of further components;
- AI models are typically integrated into AI systems;
- Specific rules apply to general-purpose AI models;
- If a provider of a general-purpose AI model integrates an own model into its own AI system, the specific rules regarding general-purpose AI models apply in addition to those applicable to AI systems;
- The specific rules do not apply when an own model is used for purely internal processes that are not essential for providing a product or a service to third parties and the rights of natural persons are not affected;
- Addition rules apply to general-purpose AI models with systemic risk.

Systemic risk

Systemic risks can, for instance, be related to major accidents, disruptions of critical sectors and serious consequences to public health and safety; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content. A general-purpose AI model is classified as "systemic risk" if:

i. It has high-impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks. This is – in any case – presumed to be the case when the cumulative amount of computation used for its training measured in floating point operations is greater than 1025;

ii. Based on a decision of the EU Commission, it has capabilities or an impact equivalent to those set out in point (i) having regard to the criteria set out in Annex XIII.

The number of parameters of the model, the quality or size of the data set, the amount of computation used for training the model measured in floating points, the input and output modalities of the model, the benchmarks and evaluations of the model, whether it has high impact on the internal market due to its reach and the number of registered end-users.

Systemic risks can vary during the lifecycle of the model, as the risk level depends on multiple factors. The following general principles should be taken into account:

- Systemic risks increase with model capabilities and model reach;
- Systemic risks can arise along the entire lifecycle of the model; and
- Systemic risks are influenced by conditions of misuse, model reliability, model fairness and model security, the level of autonomy of the model, its access to tools, novel or combined modalities, release and distribution strategies, the potential to remove guardrails and other factors.

Floating point operations

A general-purpose AI model should be considered to present systemic risks if it has high-impact capabilities: capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models. The use of floating points is one of the most relevant ways to measure model capabilities. Floating points consist of

i. Cumulative amount of computation used for training; and

ii. Methods that are intended to enhance the capabilities of the model prior to deployment, such as pre-training, synthetic data generation and fine-tuning.

An initial threshold of floating point operations is set at 1025: if met by the general-purpose AI model, it is presumed to be a general-purpose AI model with systemic risks.

Recitals 110-113 AI Act
Articles 51, 51 (1)(a)
and 52 AI Act

The assessment should be carried out by the provider himself. In individual cases, the EU Commission may take individual decisions not designating a general-purpose AI model as a general-purpose AI model with systemic risk. The current threshold of 1025 may be changed by the AI Office over time.

Designation by EU Commission

- If the systemic risk threshold as included in Article 51(1)(a) AI Act has been met, the provider shall notify the EU Commission within two weeks;
- By means of the notification, the provider may ask the EU Commission to not classify the general-purpose AI model as “having systemic risk” due to the relevant specific characteristics. If rejected, the general-purpose AI model is considered to be “having systemic risk”;
- The EU Commission will publish a list of all general-purpose AI models with systemic risk.

Requirements

The following requirements apply to providers of general-purpose AI models:

Technical documentation

- Technical documentation must demonstrate compliance with relevant requirements
- Documentation must include, for example, a general description of the AI model including the tasks intended to perform, the acceptable-use policy, the date of release, the architecture and number of parameters, the modality and, if relevant, the applicable licences
- Does not apply to AI models that are released under a free and open-source licence

Information for integrators

- Information for providers who intend to integrate the general-purpose AI model into their (own) AI systems
- Enable providers to obtain a good understanding of the capabilities and limitations of the general-purpose AI model
- The information as listed in Annex XII should be provided
- Does not apply to AI models that are released under a free and open-source licence

Copyright policy

- A policy should be put in place to ensure compliance with EU copyright law

Information about training content

- Providers of such models must draw up and make publicly available a sufficiently detailed summary of the content used for training the general-purpose AI model
- The information to be provided should be generally comprehensive in its scope instead of technically detailed to facilitate parties with legitimate interests, including copyright holders, to exercise and enforce their rights under applicable law

Appoint a representative

- Providers outside the EU should appoint a representative that is established in the EU
- The representative must be enabled to perform the tasks as specified in the provider's mandate
- The representative shall in any case verify the existence of the technical documentation, keep a copy of such documentation and cooperate with the AI Office if needed
- This also applies to regular AI systems with a high risk

Requirements for systemic-risk models

The following additional requirements apply to providers of general-purpose AI models with systemic risk:

i. Carry out evaluations to identify and mitigate systemic risks;
ii. Assess and mitigate systemic risks from the source;
iii. Keep track of and report serious incidents with the AI Office and possible national authorities;
iv. Ensure an adequate level of cybersecurity protection.

Recitals 114 and 115 AI Act
Article 55 AI Act

Link with GDPR

General Data Protection Regulation

- Although AI systems may use or otherwise process personal data, the AI Act also applies to AI systems not processing personal data. If personal data is processed, the GDPR is – of course – also of importance. The AI Act does not affect the GDPR.
- Several definitions used in the GDPR are also used in the AI Act, such as “personal data”, “biometric data” and “special categories of personal data”
- In order to facilitate compliance with the GDPR, data governance and management practices should include, in the case of personal data, transparency about the original purpose of the data collection
- Data protection impact assessments shall be carried out – by the deployer – by using information obtained from the provider

Main take-aways

Steps to take

Step 1

Define: is the application in place an “AI system” or “general-purpose AI model”?

Step 2

Purposes for application:

a) Are these purposes probihited?

b) If not, what risk category is applicable?

Step 3

What is your role: deployer, provider?

Step 4

What obligations apply to you and the AI system?

Step 5

Do you need to comply with any other relevant EU legislation?

Step 6

Implement: who is responsible for what?

Step 7

Check and re-assess!

Overview of obligations: general

Obligation	Provider	Deployer
AI literacy	●	●
Transparency towards users	●	●
Transparency towards others in the AI chain	●	

Overview of obligations: high risk

Obligation	Provider	Deployer
Have in place technical documentation	●	●
Provide information to integrators	●	
Have in place a quality management system	●	
Have in place documentation regarding, amongst others, technical specifics, the quality management system and correspondence of the notified bodies	●	
Keep and store generated logs	●	●
Carry out a conformity assessment and draw up a declaration of conformity	●	
Affix the CE-marking on the AI system	●	
Carry out fundamental rights impact assessment		●
Keep in mind cybersecurity	●	●
Appoint a representative if needed	●	

Overview of obligations: general-purpose AI models

Obligation	Provider
Ensure compliance with the AI Act	●
Include contact information on the AI system	●
Have in place a copyright policy	●
Have in place information about training and testing	●
Appoint a representative if needed	●

The team

Sara Ataei
Attorney-at-law
T: +32 484 98 55 11
M: +32 2 629 42 37
E: sataei@akd.eu

Olivier Belleflamme
Attorney-at-law
T: +32 472 03 48 93
M: +32 2 629 42 74
E: obelleflamme@akd.eu

Paul van den Bulck
Partner, Attorney-at-law
T: +32 475 52 84 08
M: +32 2 629 42 39
E: pvandenbulck@akd.eu

Jurriaan Dane
Attorney-at-law
T: +31 88 253 51 17
M: +31 6 52 61 55 54
E: jdane@akd.eu

Bente van Dijk
Attorney-at-law
T: +31 88 253 55 41
M: +31 6 57 45 60 96
E: bvandijk@akd.eu

Sophie Hendriks
Attorney-at-law
T: +31 88 253 59 54
M: +31 6 27 39 91 82
E: shendriks@akd.eu

Martin Hemmer
Partner, Attorney-at-law
T: +31 88 253 59 16
M: +31 6 27 74 27 27
E: mhemmer@akd.eu

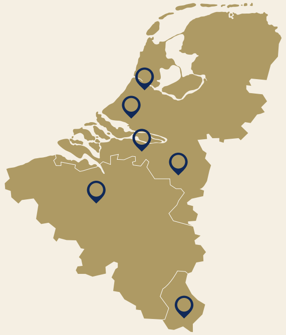
Lisa Machgeels
Attorney-at-law
T: +31 88 253 54 22
M: +31 6 21 90 01 68
E: lmachgeels@akd.eu

Renée Schipper
Counsel, Attorney-at-law
T: +31 88 253 54 05
M: +31 6 29 66 63 48
E: rschipper@akd.eu

About AKD

AKD is a major full-service Benelux law firm, with over **500 lawyers, tax advisers, civil-law notaries and business support staff** in Belgium, the Netherlands and Luxembourg. For over a century, we have combined a full-service approach and a broad sector focus to consider any question from a range of angles and provide quality solutions - anywhere in the world.

Full service
Benelux law firm



500+

Lawyers
Civil-law notaries
Tax advisors
Support

AKD
covers all important areas of law

akd

T: +31 88 253 5000
E: info@akd.eu
akd.eu