France Digitale
Jouons collectif

WAVESTONE

February 2024

AI Act

All you need to know to understand and comply with the EU law on AI

Contents

AI Act is coming!

Are you developing a solution based on Artificial Intelligence or integrating AI into your processes, products or services? Get ready, as you will need to comply with a new regulation, the AI Act.

Here's a summary of the practical consequences of this regulation ⤵

The AI Act aims to ensure that artificial intelligence systems and models marketed within the European Union are used in an ethical, safe, and respectful manner, adhering to the fundamental rights of the EU.

What will change in practice? The AI Act establishes product regulation, ranging from CE Marking to prohibition, applicable to AI systems and models being marketed. Research activities without commercial objectives are not affected.

Who needs to ensure compliance? All providers*, distributors*, or deployers* of AI systems and models, legal entities (companies, foundations, associations, research laboratories, etc.), that have their registered office in the European Union, or if they are located outside the EU, who market their AI system or model within the European Union.

Are all AI systems and models subject to "product" regulation? The level of regulation and associated obligations depend on the risk level posed by the AI system or model. There are four risk levels and four levels of compliance:

- Unacceptable risk AI: Systems and models with unacceptable risk are prohibited and can neither be marketed nor used within the European Union nor exported.
- High-risk AI: High-risk AI systems and models must receive CE Marking to be marketed.
- Low-risk AI: Low-risk AI systems and models must meet information and transparency obligations towards users.
- Minimal-risk AI: Minimal-risk AI systems and models can adhere to codes of conduct.

Special obligations apply to generative AIs and the development of General Purpose AI (GPAI), with different regulations depending on whether the model is open source or not, and other subsidiary criteria (computing power, number of users, etc.).

What is the compliance deadline? Different deadlines, ranging from 6 to 36 months, apply depending on the risk level of AI systems and models. **Regardless of the deadline, it is essential to be prepared and anticipate compliance, which may disrupt the tech, product, and legal roadmaps of companies.**

All you need to know about AI Act's compliance obligations

The compliance obligations of AI systems under the AI Act vary based on the level of risk.

	Unacceptable risk	High risk	Limited risk	Minimal risk
	These systems contravene EU values and infringe upon fundamental rights. Article 5.I provides an initial list of unacceptable high-risk AI applications, including social scoring, widespread biometric identification, deepfakes, content manipulation, and actions that harm certain population categories, etc. This list will be regularly updated by the AI Office.	**These systems are deployed in high-risk products as defined in Annex II or in high-risk sectors as defined in Annex III of the AI Act**	**These are systems that interact with individuals (Art. 52, I) and are neither of unacceptable risk nor high risk** such as artistic deepfakes or chatbots.	**These are other AI systems (not defined as unacceptable, high-risk, or limited-risk)** such as AI in video games, anti-spam filters, etc.
	Prohibition to place on the market including outside the EU	**High-risk use cases** Declaration of conformity + Registration in the EU database + CE marking	**Non-high-risk use cases*** Declaration of conformity + Registration in the EU database	**Obligation to inform** users that the content was generated by AI	**Voluntary application of codes of conduct**
	6 months after the publication of the AI Act (ie. November 2024, TBC)	**24 months (or 36 months** if the high-risk AI system is already regulated by other European legislation) after the publication of the AI Act		**24 months** after the publication of the AI Act (ie. October 2026, TBC)	**24 months** after the publication of the AI Act (ie. October 2026, TBC)
	35 million EUR ou 7% of total worldwide annual turnover (whichever is higher or lower depending on the company)	**15 million EUR ou 3% of total worldwide annual turnover** (whichever is higher or lower depending on the company)		**7,5 million EUR ou 1% of total worldwide annual turnover** (whichever is higher or lower depending on the company)	

*companies can demonstrate their AI system is not high risk

What you need to know

The compliance obligations outlined in the AI Act apply to each AI system or model individually and not to the entire company. We recommend mapping all AI systems used within your entity.

Some examples for illustration

The following are three use cases that demonstrate how risk level classification and compliance are carried out.

#1 Spam filters: a low-risk AI system

A company creates a program to prevent unsolicited, unwanted, and virus-infected emails from reaching its employees' mailboxes. The program uses algorithms to determine the probability that an email is spam or not. This type of AI system does not require a high level of compliance because this use of AI is neither at unacceptable risk, nor at high risk, nor at low risk as defined in the AI Act. However, it is recommended to establish a code of conduct for AI systems. This code of conduct should be developed based on clear objectives and key performance indicators to measure the achievement of its goals. Requirements could include elements such as fairness, transparency, confidentiality, and sustainability. This code of conduct can also apply to multiple AI systems within the company if they have a similar purpose.

#2 Artistic deep fakes: a low-risk AI system

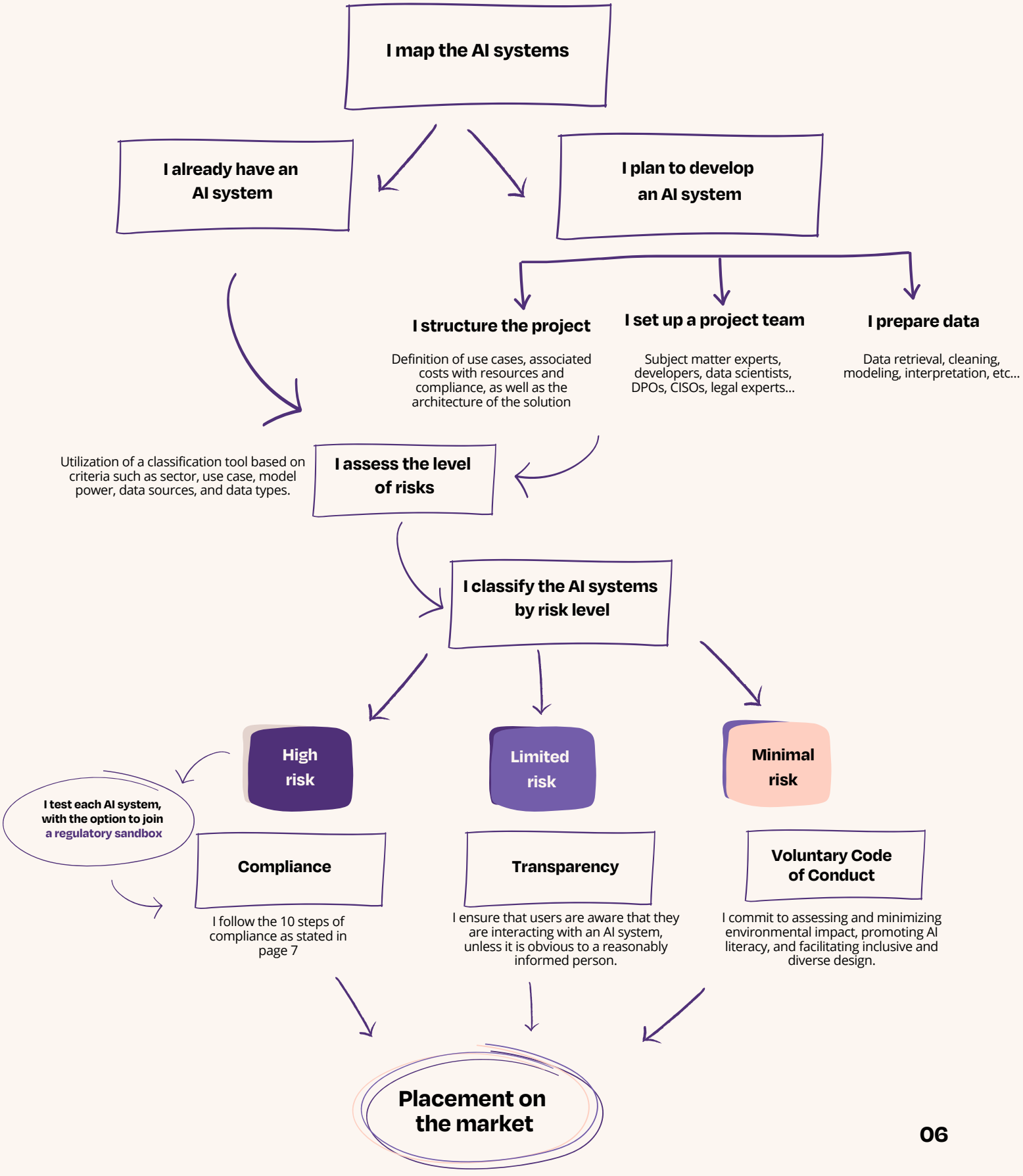
As a production company, you want to create a video lesson on quantum physics with AI-generated image of Einstein to animate the video. It is imperative to explain that the content was created using this technology. Therefore, you should add information or a warning in the video to explain that the image was generated by AI (the choice of wording is free to avoid hindering the display or the content itself). This will allow learners to understand that Einstein's image is generated by a machine.

#3 Credit scoring: a high-risk AI system

You are a financial institution that wants to create an AI system to assess the creditworthiness of loan applicants. You have access to sensitive customer data (credit history, income, employment), and based on this, your algorithms determine whether a loan should be granted and under what conditions. Your use case is considered high-risk because it can be discriminatory. To be able to market your AI, you must commit to the compliance process.

How to ensure the compliance of your existing and future AI systems?

The AI Act applies to both existing (legacy) systems and new solutions. You will find below a standard guide to help you understand what you need to do to be compliant.



🔍 The 10 steps of compliance for high-risk AI systems

☐ **Risk Management System**	I adopt appropriate and targeted risk management measures to address identified risks.
☐ **Data and Data Governance**	I use high-quality training data, adhere to appropriate data governance practices, and ensure that datasets are relevant and unbiased.
☐ **Technical Documentation**	I include the specified minimum elements outlined in Annex IV.
☐ **Traceability**	I ensure that records are available throughout the lifespan of the AI system, with tracking designed for traceability and transparency.
☐ **Human Supervision**	I incorporate human-machine interface tools to prevent or minimize risks upfront, enabling users to understand, interpret, and confidently use these tools.
☐ **Accuracy, Robustness and Security**	I ensure consistent accuracy, robustness, and cybersecurity measures throughout the AI system's lifecycle, with declared precision metrics, resilience against errors, and appropriate measures to address potential biases.
☐ **Quality Management System**	I draft and document a quality management system covering regulatory compliance, design, development, testing, risk management, post-market surveillance, incident reporting, communication, data management, record retention, resource management, and accountability.
☐ **EU Declaration of Conformity**	I draft the declaration of conformity, which is clear and signed, for each high-risk AI system, asserting compliance with the requirements of Chapter 2. I keep it up to date for 10 years, submit copies to national authorities, and update it as necessary.
☐ **CE Marking**	I ensure that the CE marking is affixed in a visible, legible, and indelible manner or digitally accessible for digital systems, thereby indicating compliance with the general principles and applicable Union laws.
☐ **Registration**	Before placing the AI solution on the market or putting it into service, I register the company as well as the system in the EU database mentioned in Article 60.

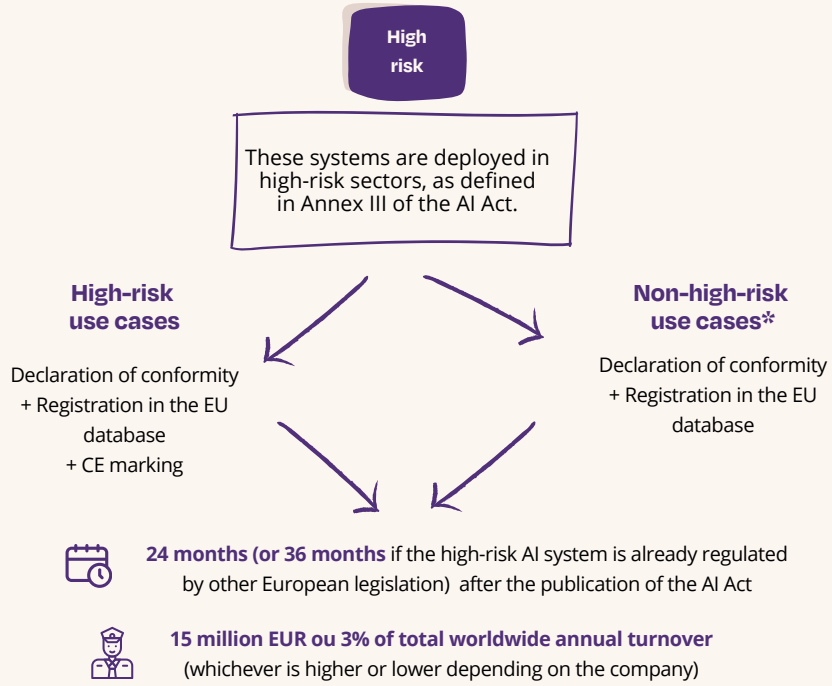
Case Study: application of the compliance Process to human resources, a high-risk AI system

TechInnovate is a fictional company with the ambition to develop an AI solution to facilitate and optimize the candidate pre-selection process. Here, we applied our compliance process:

- The company **identifies use cases for its new AI system,** including automatic CV analysis, automated virtual interviews, and post-interview feedback analysis.
- **The estimated project cost is approximately €60,000**, considering the need to involve an HR expert, a cybersecurity and data protection expert, three data scientists, a project manager for one month, and a lawyer for two days to support compliance.
- TechInnovate **collects data** about candidates' professional experience, technical skills, references, and interviews, and models this information.
- To **assess risks**, the company uses a tool that considers the industry (human resources), data sensitivity (individual skills and performance), and the complexity of the AI model.
- TechInnovate's recommendation engine is **classified as presenting a high risk** due to the use of personal and sensitive data to enhance recruitment efficiency, with the potential risk of algorithmic biases influencing decisions.
- To address these risks, TechInnovate decides to **test its AI system in a regulatory sandbox** to ensure in particular the absence of biases. To this end, TechInnovate must respect all the conditions set by the competent, national authority, which enables the company to test its AI system in a regulated and controlled environment without violating the applicable regulations.
- Subsequently, TechInnovate **undertakes the compliance of its AI system in accordance with the AI Act**. This process includes implementing privacy and data security policies to manage risks, respecting data governance standards, integrating specified measures specified in Annex IV, preserving model training records, ensuring model accuracy, system robustness, and implementing cybersecurity measures, as well as establishing a quality management system.
- TechInnovate **thoroughly documents** how each requirement of the AI Act is met in its compliance statement. After completing all compliance steps, TechInnovate submits its **declaration of conformity** to the competent authorities, obtains the CE marking, and then registers it in the EU database.
- Now able to **market its enhanced recommendation system**, TechInnovate highlights its **CE marking**, reinforcing customer trust in the compliance of its AI solution.

Focus on High-Risk AI

Let us remind you how the regulation for high-risk AI operates:



Here are the steps to follow

1 - Determine if the AI system or model is deployed in a high-risk sector

To determine if an AI system is high-risk according to the AI Act, it is necessary to check whether it is listed in the Annex II and Annex III of this regulation. Annex III of the AI Act defines 8 major areas of activities identified as 'high risk':

1. Remote biometric identification and categorisation
2. Critical infrastructure
3. Education and vocational training
4. Employment, workers management and access to self-employment
5. Access to and enjoyment of essential private services and essential public services and benefits
6. Law enforcement
7. Migration, asylum and border control management
8. Administration of justice and democratic processes

2 - Initiate the Compliance Process (i.e., CE Marking)

All high-risk AI systems will be assessed before they are placed on the market and throughout their lifecycle. Concerned companies must obtain CE Marking to market their solution unless they can demonstrate that the use of the AI system or model is not inherently high-risk.

You must then follow the compliance checklist detailed on page 7.

3 - Unless you can demonstrate your AI system is not high-risk

For AI systems covered by Annex III, AI systems are not considered high-risk if the following cumulative conditions are met:

- The AI system does not create a significant risk to the health, safety, or fundamental rights of individuals;
- The AI system does not substantially influence the outcome of decision-making.

This will be the case, in particular, if the AI system is intended for a limited procedural task, or to enhance the result of a previously completed human activity, or to detect decision-making patterns or deviations from previous decision-making models, and is not intended to replace or influence prior human evaluation without appropriate human review, or to perform a preparatory task.

Note that an AI system shall always be considered high-risk if the AI system performs profiling of natural persons.

If the AI system is not considered high-risk by the company, the latter must perform the following tasks:

- Document its risk assessment
- Register the system in the EU database
- Be available for inspection by the national authority if required

Important: There is significant legal uncertainty for this procedure.

Gide's perspective: Focus on AI Systems Integrated as Safety Components of Products Already Covered by other European sector-specific legislation (Annex II)

GIDE
GIDE LOYRETTE NOUEL

Among the AI systems considered high risk, the AI Act lists various AI systems integrated as safety components in products already subject to sector-specific legislation (Annex II). These are products already subject to specific requirements and compliance testing before they can be placed on the market. The targeted use cases are diverse, including AI systems used as safety components in children's toys, medical devices, elevators, and more.

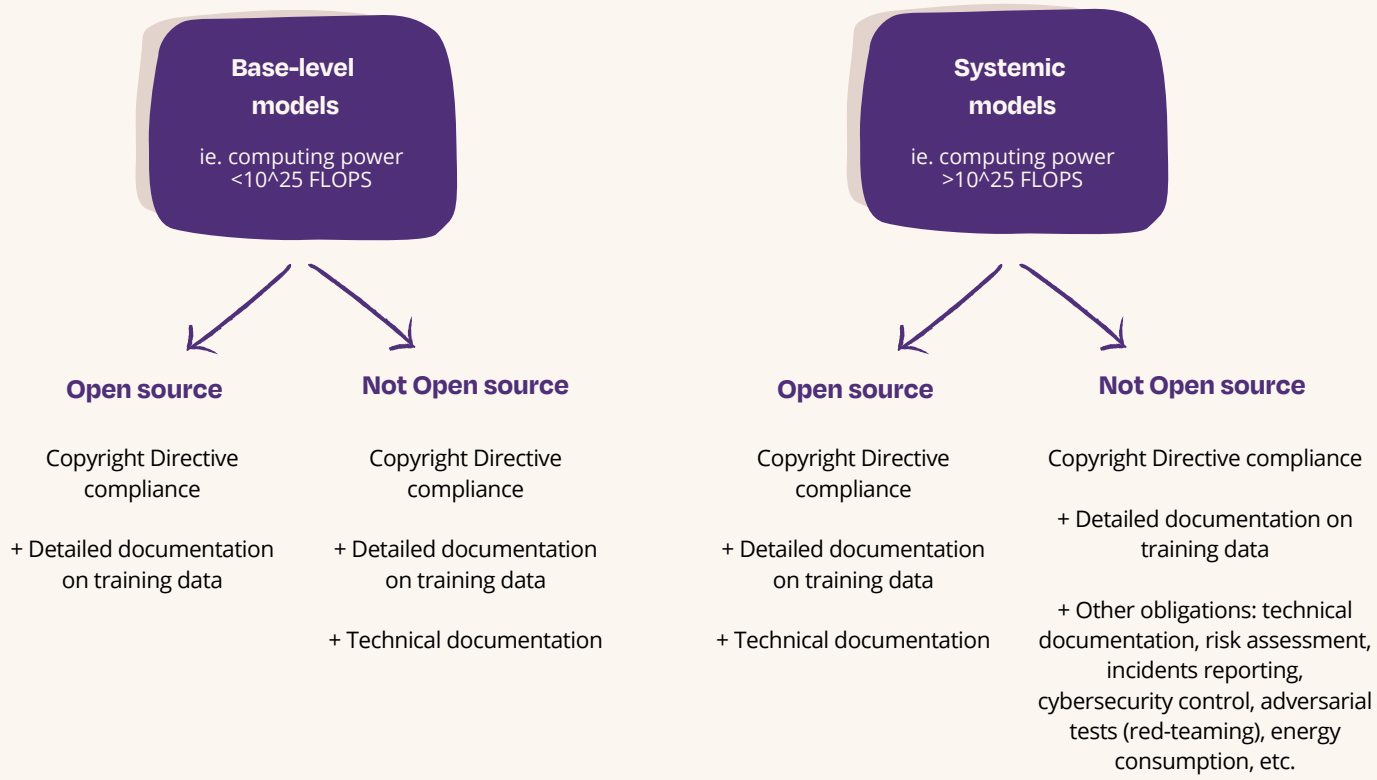
These systems must comply with all obligations outlined in the AI Act for high-risk AI systems, as well as the requirements from the sector-specific legislation applicable to the product in which the AI system is incorporated.

With the aim of ensuring better consistency between the requirements of different regulations and attempting to limit the burden associated with the cumulative application of the AI Act and the sector-specific legislation applicable to the targeted product:

- The AI Act stipulates that the supplier can integrate the necessary measures to comply with the AI Act into the procedures and documents already required by the sector-specific legislation.
- The compliance deadline for the AI Act is extended: companies must be compliant with the AI Act within 36 months following the entry into force of the text.

Focus on Generative AI and General-Purpose AI Models (GPAI)

Compliance obligations for General Purpose AI Models (GPAIs) depend on whether the model is open source or not, as well as subsidiary criteria, including computing power exceeding or falling below 10^25 FLOPS.



What you need to know

The classification as a General Purpose AI Model or as a General Purpose AI Model *with systemic risk*. To date, only the criterion of computing power (> or < 1025 FLOPS) has been established. The AI Office may decide to add additional criteria, such as the number of business users.

The classification of the model as open source or not. Article 52c defines open-source AI models as models that are made accessible to the public under a free and open licence that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available.

Still pending clarifications on the obligations for GPAI with systemic risk: The AI Office will work on developing codes of practice and a methodology to determine whether a general-purpose AI model (GPAI) should be considered as having systemic risk and to assist developers, distributors, and deployers of models such as LLMs in complying with the requirements and obligations of the AI Act.

Copyright, datasets and generative AI: All GPAI models, whether open source or not, must provide a summary of training data and are subject to copyright legislation.

Gide's perspective: clarification on AI, data protection and copyright

GIDE
GIDE LOYRETTE NOUEL

More and more rules determining access to dataset

Training AI models and systems may rely on data and content that is protected or subject to specific rules. In this regard, the AI Act intersects with other existing legislation. In particular, the GDPR for personal data and other laws related to copyright and related rights. The use of data by AI systems and models must therefore comply with all these legal texts. Regarding personal data, two points require special attention to determine the obligations applicable to the data controller: the purpose of data processing (the objective pursued by the use of data) and the conditions for data collection and retrieval.

Copyright compliance by providers of general-purpose AI models

For general-purpose AI models (amongst which LLM), the new European framework aims to create a balance between the need for content to train models and the protection of content through copyright law. Thus, the AI Act imposes on providers of general-purpose AI models (e.g. LLMs) the obligation to establish procedures to ensure compliance with copyright law regarding the content used by the model. The fact that right holders can object to the mining and automated analysis of data (so-called "opt-out" system) suggests that negotiations for a balanced sharing of the value generated through the use of copyrighted content by AI systems are to be expected in the near future. Providers of general-purpose AI models will be subject to transparency obligations regarding the sets of content used to train their models. The principles set forth by the regulation call for the designation of harmonized technical standards for the identification of content, and the definition of relevant business models for a fair value-sharing arrangement.

Anticipating compliance before market entry: regulatory sandboxes and testing in real world conditions

Anticipating market access with regulatory sandboxes

The AI Act establishes an obligation for each national authority to deploy, at the level of one or more Member States, a regulatory sandbox.

These regulatory sandboxes are intended to be operational at the time of the AI Act's implementation in 2026. They are designed to allow providers to develop, train, test, and validate AI systems for a specified period before market entry. This collaborative process involves working with competent national authorities to ensure compliance with the AI Act.

Conceived to support innovation and competitiveness among European stakeholders, these sandboxes aim to facilitate market access for AI systems developed by European startups and SMEs.

Based on technical standards to be published by the European Commission, national authorities will need to specify the eligibility criteria and operational conditions for these regulatory sandboxes.

Beyond regulatory sandboxes: testing in real world conditions

In addition to regulatory sandboxes, the AI Act also enables AI system providers to conduct testing in real world conditions of their AI systems without violating the AI Act, provided certain specific conditions are met.

Among these conditions, there is the requirement to obtain approval from the competent national authority based on a test plan submitted by the provider in advance. This plan should specify a defined testing duration and require that individuals involved in the tests are duly informed and give their consent.

Forthcoming technical standards from the European Commission are expected to harmonize the conditions under which these real-world testing facilities will be implemented in each Member State.

Key dates to be ready on Day 1

The AI Act will apply gradually based on the risk level of AI systems or models, as summarized here:

Important : The deadlines set by the legislator start from the date of entry into force of the AI Act (which is 20 days after the publication of the text in the Official Journal of the European Union) and will be specified as soon as the official publication date is known.

While this progressive timeline has been designed by the regulator to give companies enough time to comply, it is crucial to anticipate the next steps.

Risks and fines for non-compliance

- Fines for a company marketing a prohibited AI system or model can go up to 7% of global worldwide turnover or 35 million EUR, whichever is higher.
- Fines for companies failing to comply with the compliance requirements for high-risk AI systems can go up to 3% of global worldwide turnover or 15 million EUR, whichever is higher .
- The supply of incorrect, incomplete or misleading information is subject to fines of up to 1 % of the total worldwide annual turnover or 7.5 million EUR, whichever is higher.

Important: For SMEs, including startups, the opposite logic applies: fines will be up to the percentages or the amounts referred above (35, 15 or 7.5 million EUR), whichever of the two is lower.

Points of contact

You should rely on three primary points of contact :

- **Two national authorities**, yet to be designated in France, responsible for (i) ensuring the effective implementation of the AI Act and the coordination with other national and European authorities, (ii) supervising the national sandbox, and (iii) exercise control and impose fines. **These authorities will be your privileged points of contact if you have questions about the implementation of the AI Act or intend to join the national sandbox.**

- The **AI Office**, integrated into the European Commission, composed of independent experts and soon to be designated. The AI Office will be responsible for (i) developing methodologies for evaluating AI models and (ii) monitoring security risks associated with general purpose AI models, in coordination with national authorities. **The AI Office will be your primary point of contact for submitting a declaration of conformity if you have a high-risk AI system or model.**

Other bodies you can rely on:

- The **AI Board**, comprising representatives from EU Member States, will coordinate the application of the text at the European level, in coordination with future national authorities.

- The **AI Advisory Forum** is a body representing civil society, including businesses, which will be regularly consulted by the AI Office to provide feedback on the implementation of the AI Act and anticipate regulatory developments over time.

- The **AI Pact** is an initiative by the European Commission that encourages companies to make voluntary commitments before the AI Act enters into force. Specifically, companies can sign a pledge to comply with the future AI law, and detail the specific actions taken for this purpose. They can also share their best practices. Participation in the AI Pact should provide easier access to European supercomputers. Participation in the AI Pact is open to all, subject to acceptance of the application. A preliminary list of participants will be published in the first half of 2024. You can participate here.

Glossary

Artificial Intelligence system: Machine-based system 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.

Compliance: Deployment of preventive procedures that allow companies to avoid exposing themselves to risks related to non-compliance with regulations. The implementation of a compliance policy allows the company to better manage risks and avoid exposure to financial and reputational risks. (French Competition Authority).

Deep fake: AI generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful.

Deployer: Any 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.

Distributor: Any 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.

General-purpose AI system: AI system which is based on a general purpose AI model, that has the capability to serve a variety of purposes, both for direct use, as well as for integration in other AI systems.

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 them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.

Regulatory Sandbox: Concrete and controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, where appropriate in real world conditions, an innovative AI system, pursuant to a sandbox plan for a limited time under regulatory supervision.

Standard: Launched at the initiative of market stakeholders, a standard is a reference framework aimed at providing guidelines, technical or qualitative specifications for products, services, or practices in the interest of the general public. It is the result of a consensual co-production between professionals and users who have engaged in its development. Standards shall be grouped into two main categories: vertical standards (sector-specific, such as automotive, aerospace, banking, etc.) and horizontal standards (more technological, such as cyber, AI, etc.).

THANKS to the contributors

Marianne TORDEUX-BITKER
Directrice des affaires publiques

France Digitale

marianne@francedigitale.org

Chadi HANTOUCHE
Partner

Wavestone

chadi.hantouche@wavestone.com

Julien GUINOT-DELÉRY
Associé - Propriété intellectuelle, Médias & Technologies

Gide

guinot@gide.com

Agata HIDALGO
European Affairs Manager
France Digitale

agata@francedigitale.org

Florence ESPITALIER
Senior Consultant

Wavestone

florence.espitalier@wavestone.com

Matthieu LUCCHESI
Counsel
Innovation & FinTech

Gide

matthieu.lucchesi@gide.com

Thomas BARREAU
IA & standardisation

France Digitale

ap@francedigitale.org

Raya CHAKIR
Consultant

Wavestone

raya.chakir@wavestone.com

Disclaimer - Important information

This guide has been prepared based on the compromise reached on the AI Act on January 29, 2024, and which was voted on in Coreper on February 2, 2024. The compromise is expected to be voted on as is in the plenary session of the European Parliament by April 2024. The AI Act will only come into effect 20 days after its official publication in the Official Journal of the European Union. The information provided in this guide may therefore vary slightly from the final adopted version of the text. This guide does not constitute legal advice, and we encourage you to seek the assistance of experts for operational compliance.

A guide produced in collaboration with

About France Digitale

Founded in 2012, France Digitale is the largest startup association in Europe, bringing together over 2000 startups and investors (venture capitalists and business angels).
The association's goal is to help build Europe's future tech champions by uniting and raising the voice of those who innovate to change the face of the world.
France Digitale is co-presided by Frédéric Mazzella, Chairman and founder of BlaBlacar, and Benoist Grossmann, CEO of Eurazeo Investment Manager.

About Wavestone

Wavestone, an independent leading French consulting pure-player, and Q_PERIOR, a consulting leader in the Germany-Switzerland-Austria region, joined forces in 2023 to become the most trusted partner for critical transformations.
Drawing on more than 5,500 employees across Europe, North America and Asia, the firm seamlessly combines first-class sector expertise with a 360° transformation portfolio of high-value consulting services.

About Gide

Gide is a French business law firm with an international dimension. Founded in Paris in 1920, the firm now operates out of 11 offices worldwide. It numbers 500 lawyers drawn from 35 different nationalities, recognised as among the most respected specialists in each of the various sectors of national and international business law.