

Artificial intelligence

JUNE 2024

A challenge for companies and for regulators



Andy Ramos

Partner, Digital Law

aramos@perezllorca.com

+34 91 423 20 72



Raúl Rubio

Partner, Digital Law

rrubio@perezllorca.com

+34 91 353 45 59



Adolfo Mesquita Nunes

Partner, Digital Law

adolfoemesquitಾನunes@perezllorca.com

+351 912 585 103

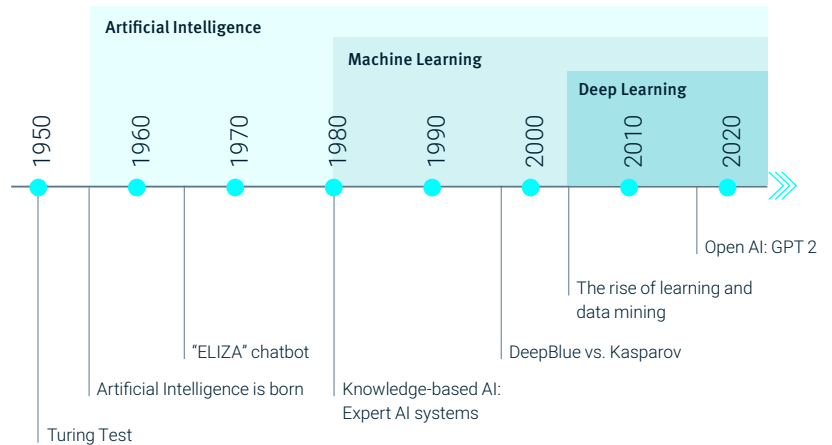
ANDY RAMOS, RAÚL RUBIO, ADOLFO MESQUITA NUNES, FRANCISCO RIBEIRO FERREIRA AND ISABEL IGLESIAS

The first Artificial Intelligence Act is here. Key aspects

1. Introduction

In the digital era, Artificial Intelligence (“AI”) has become a central element of innovation and technological development, bringing about significant transformations in all sectors of the economy and society. The enormous potential of AI has been perceived by certain regulators as a threat to citizens' rights and freedoms, prompting debates on the responsible and ethical development and use of this technology, and proposals to regulate potential conflicts before they even arise.

For more information on general aspects of AI, we recommend reading the first in this series of publications, available [here](#).



Evolution of artificial intelligence

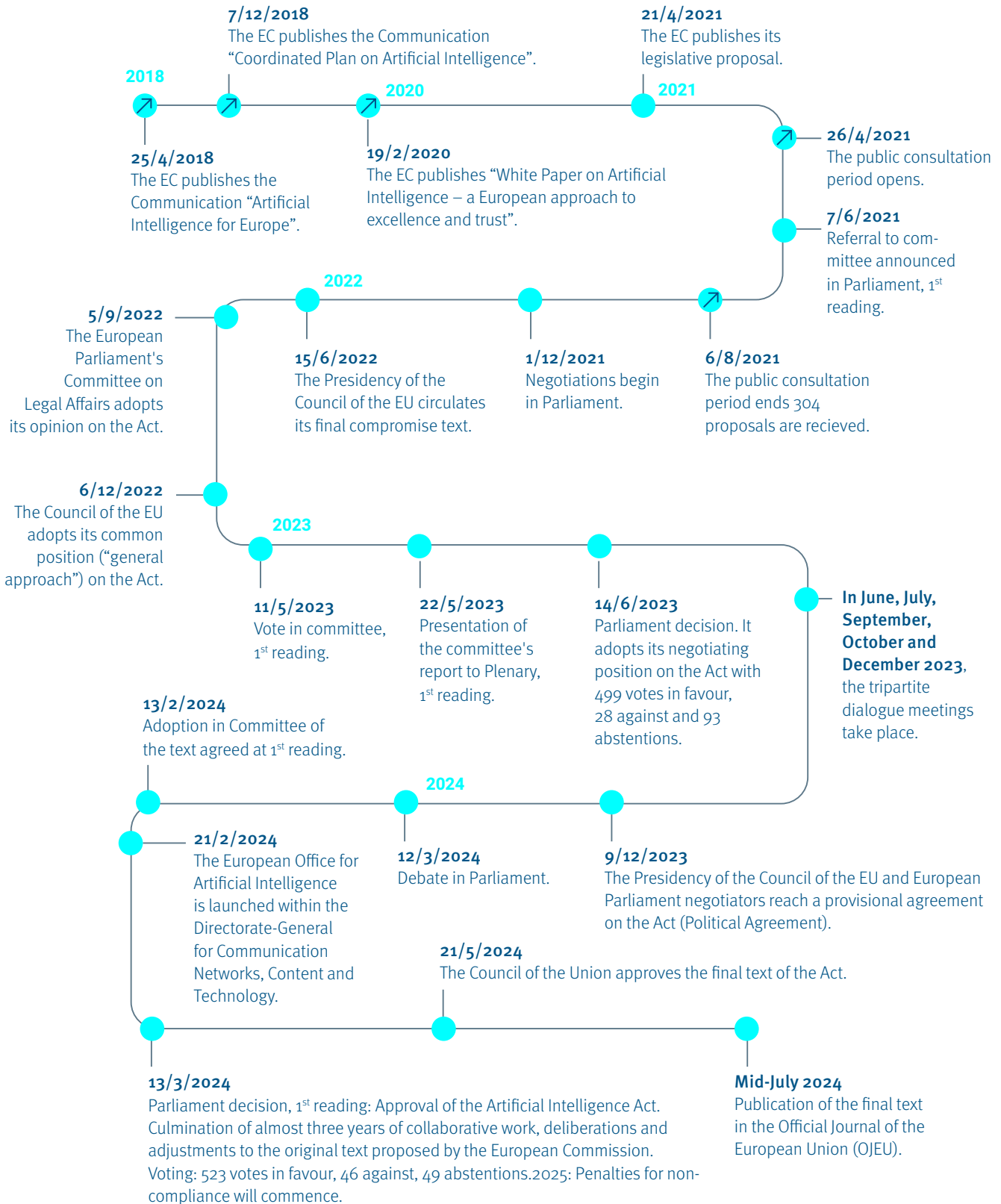
On 13 March, the European Union (“EU”) adopted the Artificial Intelligence Act (the “Act”), a legislative framework aimed at establishing harmonised rules on AI within Member States. The European regulator intends the Act to become a part of an AI ecosystem that is safe, reliable and aligned with European values and principles. In doing so, the EU seeks to position itself as a leader in establishing a comprehensive regulatory framework for AI, which not only addresses the risks associated with its use, but also promotes its ethical and humane development.

This Act, the result of a long legislative process, formally endorses a balanced approach that seeks to promote innovation and technological development, while ensuring the protection of the health, safety and fundamental rights of European citizens. However, as we will see, the control measures in the Act far outweigh the promotion measures, the latter being much more vague and underdeveloped compared to the level of specificity of the former, which is inconsistent with the recitals of the Act and with the current incipient state of AI.

This legal briefing aims to provide an analysis of the most significant aspects of the adopted text, the legal and business implications, and some practical recommendations on how to adapt the economic activity of any company affected by the Act.

2. Timeline of the Act

Developing and approving the Act has been a complex and painstaking process, given the innovative nature of the regulations and the technology itself, as well as the importance and potential impact of AI on society. The timeline of key events leading up to the recent adoption of the Act is as follows:



3. Purpose of the Act

The stated purpose of the Act is to improve the functioning of the internal market by laying down a uniform legal framework for the development, placing on the market, putting into service and use of AI systems in the EU.

The Act seeks to promote the adoption of human-centred and reliable AI, while ensuring a high level of protection of health, safety and fundamental rights, and to support innovation. In addition, it establishes harmonised rules for putting AI systems on the market, prohibitions on certain AI practices, specific requirements for high-risk AI systems, transparency rules and measures to support innovation.

“The Act seeks to balance the promotion of innovation and technological development with the need to ensure that AI is developed and used in a way that respects the fundamental rights and values of the European Union.”

Furthermore, Recital 27 of the Act highlights the importance of a risk-based approach to establish effective and proportionate rules, also highlighting the 2019 Ethics Guidelines for Trustworthy AI, which were drafted by the independent High Level Expert Group on AI appointed by the Commission. The Group proposed seven non-binding core ethical principles to promote the reliability and ethics of AI. These principles include: human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability. These guidelines, while not legally binding, complement the requirements of the Act.

ESSENTIAL ETHICAL PRINCIPLES:	
 Human agency and oversight	 Transparency, diversity, non-discrimination and fairness
 Technical robustness and safety	 Societal and environmental well-being
 Privacy and data governance	 Accountability

4. The AI Act in figures



180 recitals



113 articles



107,000+ words



13 chapters



13 annexes



20 delegated and implementing acts

5. Scope of the Act

The Act will apply to:	It will not affect:
<ul style="list-style-type: none">Providers placing on the market or putting into service AI systems or AI models for general use in the Union, irrespective of their location.	<ul style="list-style-type: none">Areas outside the scope of EU law.
<ul style="list-style-type: none">Deployers of AI systems that have their place of establishment or are located within the Union.	<ul style="list-style-type: none">Member States' competences concerning national security.

The Act will apply to:	It will not affect:
<ul style="list-style-type: none"> Providers and deployers of AI systems located in third countries when the output is used in the Union. 	<ul style="list-style-type: none"> AI systems that are used exclusively for military, defence or national security purposes, regardless of the type of entity conducting these activities.
<ul style="list-style-type: none"> Importers and distributors of AI systems 	<ul style="list-style-type: none"> Public authorities of third countries and international organisations when using AI systems in the framework of international cooperation or agreements for the purposes of law enforcement and judicial cooperation with the Union or with one or more Member States, provided that it offers sufficient safeguards with respect to the protection of fundamental rights and freedoms of individuals.
<ul style="list-style-type: none"> Product manufacturers placing on the market or putting into service an AI system together with their product. 	<ul style="list-style-type: none"> The application of the provisions on the liability of intermediary service providers set out in Chapter II of Regulation (EU) 2022/2065.
<ul style="list-style-type: none"> Authorised representatives of providers not established in the Union. 	<ul style="list-style-type: none"> AI systems or models developed and put into service for the sole purpose of scientific research and development.
<ul style="list-style-type: none"> Affected persons located in the Union. 	<ul style="list-style-type: none"> Any research, testing or development activity relating to AI systems or AI models prior to their being placed on the market or put into service.
<ul style="list-style-type: none"> Article 112 will only apply to high-risk AI systems, while Article 57 will only apply to the extent that the requirements for high-risk AI systems have been integrated into such Union harmonisation legislation. 	<ul style="list-style-type: none"> The obligations of deployers who are natural persons using AI systems in the course of a purely personal non-professional activity.
<ul style="list-style-type: none"> AI systems released under free and open source licences that fall within the scope of Article 5 (prohibited practices) or Article 50 (practical application of transparency obligations). 	<ul style="list-style-type: none"> In general, AI systems released under free and open source licences, apart from the exceptions mentioned.

6. Definition of an artificial intelligence system

According to Article 3(1) of the Act, an AI system is “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.”

With this wording, the European legislator aims to make its conceptualisation of AI sustainable over time, which requires it to encompass an exceptionally wide range of data analysis techniques, and to be applicable to a wide variety of technologies currently used in the business sector and in public administration.

7. Categorisation of AI systems

The categorisation of AI systems under the Act focuses on the concept of risk¹, classifying such systems according to the level of risk they pose to society, security, fundamental rights and human welfare. **The Act mainly regulates high-risk AI systems**, and sets out detailed requirements for their development, deployment and use. The following types of AI systems are identified:

¹ According to Article 3(2) of the Act, “risk” is the combination of the probability of an occurrence of harm and the severity of that harm.

- **Prohibited AI systems:** Some AI applications are prohibited because of the unacceptable risks the legislator considers they present in relation to fundamental rights and freedoms. This includes mass surveillance systems and systems that manipulate human behaviour to circumvent people's autonomy; exploiting vulnerabilities of a specific group of people due to their age or disability; conducting social assessments of behaviour in social and public settings; and the use of social credit scores by public authorities, among other things.
- **High-risk AI systems:** AI systems are considered high risk when they are likely to affect the fundamental rights of individuals or their security in a significant way. These systems are subject to strict regulatory requirements, including risk management systems, conformity assessments, high standards of transparency, technical documentation prior to market introduction, mandatory record-keeping, human oversight requirements, and strong data protection and cybersecurity safeguards.
- **Limited-risk AI systems or those with special transparency obligations:** the Act includes provisions related to transparency and the provision of adequate information to users. This includes requirements for AI system providers to clearly inform users when they are interacting with an AI system, ensuring that people are aware of the automated nature of the interaction.

8. Prohibited AI practices








The Act establishes a number of prohibited practices in relation to AI systems, such as placing on the market, putting into service or using:




- **Subliminal and manipulative techniques:** AI systems that use subliminal or manipulative techniques with the aim of significantly altering people's behaviour in a way that impairs their ability to make informed decisions.
- **Exploitation of vulnerabilities:** AI systems that exploit vulnerabilities of specific individuals or groups, based on their age, disability or socio-economic situation, in order to materially distort their behaviour in a way that may cause them significant harm.
- **Social credit systems:** AI systems to evaluate or rank individuals or groups over time based on their social behaviour or personal or personality characteristics, resulting in detrimental or unfavourable treatment in contexts unrelated to the data collected.
- **Individual predictive policing:** AI systems specifically designed to assess the risk of a person committing a criminal offence, based solely on profiling the person or assessing their personality traits. AI systems that support the assessment of a person involved in criminal activities are exempted, provided that this assessment is based on objective and verifiable facts.
- **Facial recognition and databases:** the creation or expansion of facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage is prohibited due to privacy implications and the potential for mass surveillance.
- **Emotional inference systems in work and education:** the use of AI systems designed to detect emotions or intentions of individuals in work or education is prohibited, except when used for medical or safety reasons.
- **Biometric identification systems in public areas:** with certain exceptions, real-time remote biometric identification systems in publicly accessible areas for the purpose of law enforcement.

9. High-risk systems

High-risk AI systems are those that represent significant potential for harm to people's safety, health or fundamental rights. For this reason, high-risk systems are subject to particularly intense scrutiny under the Act, to ensure that they are implemented in a safe and reliable manner.

9.1. Classification

 <p>Biometrics</p>	<ul style="list-style-type: none"> » Remote biometric identification systems. Exclusion: when the sole purpose is to confirm the identity of the person. » AI systems for biometric categorisation according to sensitive or protected attributes or characteristics. » AI systems for emotion recognition.
 <p>Critical infrastructure</p>	<ul style="list-style-type: none"> » AI systems as safety components in the management and operation of critical digital infrastructure, traffic, water supply, gas, heating or electricity.
 <p>Access to essential private services and essential public services and benefits</p>	<ul style="list-style-type: none"> » AI systems used by public authorities to evaluate eligibility for essential services and benefits, including healthcare. » AI systems to evaluate creditworthiness, credit rating, insurance risk and pricing, and evaluating and classifying emergency calls.
 <p>Migration, asylum and border control management</p>	<ul style="list-style-type: none"> » AI systems used by competent authorities for risk assessment (security, health, irregular migration), examination of asylum applications, visa, residence permits, and the detection, recognition or identification of persons.
 <p>Safety of regulated products</p>	<ul style="list-style-type: none"> » AI systems which are intended to be used as a safety component of a product falling within the scope of Union harmonisation legislation (listed in Annex I of the Act) or where the AI system itself is such a product (Machinery Regulation, Toy Safety Directive...). » An AI system is not considered to be high-risk if it does not pose a significant risk of causing harm to the health, safety or fundamental rights of natural persons, in particular by not materially influencing the outcome of decision making. This is the case when its use is limited to: (i) performing a specific procedural task; (ii) improving the result of a previously completed human activity; (iii) detecting decision-making patterns without influencing human assessments without an adequate review; (iv) performing a preparatory task to an assessment relevant to the listed use cases.
 <p>Education and vocational training</p>	<ul style="list-style-type: none"> » AI systems to determine access/admission or to assign individuals in educational and vocational training institutions. » AI systems to evaluate learning outcomes or the appropriate level of education. » AI systems for monitoring and detecting prohibited behaviour during tests.
 <p>Employment, workers management and access to self-employment</p>	<ul style="list-style-type: none"> » AI systems for recruitment, selection, analysis and filtering of job applications, evaluation of candidates. » AI systems for decisions affecting working conditions, promotion, termination of employment relationships, assignment of tasks, performance monitoring and evaluation.

 <p>Law enforcement</p>	<ul style="list-style-type: none"> » AI systems to assess the risk of becoming the victim of a criminal offence, reliability of evidence, likelihood of offending or re-offending, and profiling during the detection, investigation or prosecution of criminal offences.
 <p>Administration of justice and democratic processes</p>	<ul style="list-style-type: none"> » AI systems for judicial assistance in interpreting facts and the law, and applying the law, or for use in alternative dispute resolution. » AI systems to influence elections or voting behaviour. <i>Exclusion: administrative or logistical tools for political campaigns.</i> » Products of which the AI system is a safety component, or when the AI system itself is a product, must undergo a third party conformity assessment for placing on the market or putting into service in accordance with the Union harmonisation legislation listed in Annex I of the Act.
 <p>An AI system will always be considered as high-risk when it performs profiling of natural persons (under Article 6 <i>in fine</i>).</p>	

9.2. Obligations of high-risk AI systems

In order for these systems to operate in the EU market, they must comply with the following requirements:

- **Conformity assessment:** before being placed on the market or put into service, these systems must undergo a conformity assessment to verify that they meet all the safety and performance requirements of the Act. This includes extensive testing to validate the accuracy, robustness and safety of the system.
- **Transparency and information:** providers must ensure that documentation of high-risk AI systems is detailed and accessible. This includes information on the methodology, algorithms, design decisions, and the capabilities and limitations of the system, therefore enabling full transparency on how the system operates and the data it uses. They must also provide users with clear and adequate information on the capabilities and limitations of the system.
 - » **Risk management:** they must establish and document a risk management system, systematically and continuously throughout the life cycle of the high-risk AI system. It must include the identification, analysis, estimation and evaluation of known and foreseeable risks and the adoption of appropriate risk management measures to address them.
 - » **Data quality:** they must ensure that the data sets used for training, testing and validation are relevant to the purpose of the system, representative, free of errors and biases, through appropriate data governance policies.
 - » **Technical documentation:** they must keep technical documentation demonstrating the conformity of the AI system with the requirements.
 - » **Activity logs:** a record of the operations of the AI system must be kept to ensure the traceability of its results. In addition, high-risk AI systems must technically allow for the automatic recording of events (log files) throughout their life cycle.
- **Instructions and information:** systems must be accompanied by instructions for deployers with complete and clear information that is relevant and understandable.
- **Provider identification:** providers of high-risk AI systems must indicate on the system, on its packaging or on its accompanying documentation, their name, registered trade name or trade mark, and their contact address.
- **Human oversight:** human oversight must be in place to minimise risk and allow intervention in the event of system malfunction to mitigate the risks of erroneous or harmful autonomous decisions. Operators must be trained and have the necessary authority to supervise and, if necessary, intervene or deactivate the AI system.
- **Cooperation with authorities:** providers of high-risk AI systems should cooperate with regulatory authorities and provide all information necessary to demonstrate the system’s compliance with legal requirements. This also includes providing access to records and documentation of the system when required by the competent authorities.
- **Robustness and accuracy:** they should ensure that the AI system is robust, accurate and capable of handling errors or inconsistencies during operation.

- **Cybersecurity:** adequate measures should be implemented to ensure cybersecurity and system integrity. In particular, measures can be implemented to prevent and respond to manipulation of training data (data poisoning), of pre-trained components used in training (model poisoning), inputs designed to cause the AI model to make a mistake, confidentiality attacks, etc.
- **Notification and registration:** the high-risk AI system must be registered in an EU database before being placed on the market (see section 9.3).

Some obligations apply to certain operators:

- **Verification of conformity:** Distributors and other operators along the value chain (such as importers and deployers) have specific obligations, such as verifying the conformity of the system before placing it on the market, ensuring proper storage and transport conditions, and taking action in the event they detect non-conformities or risks.
- **Verification of impact on fundamental rights:** they must ensure that the use of the AI system does not lead to discrimination and that it is respectful of fundamental rights.
- **Authorised representative:** before placing a high-risk AI system on the EU market, providers established in third countries must appoint, by means of a written mandate, an authorised representative which is established in the EU.

In short, high-risk AI systems are subject to a detailed regulatory framework that requires compliance at multiple levels, from the validation of their technology to the management of the data they process. These measures aim to protect individuals and society from the potential harm that these powerful systems could cause if not properly managed.

9.3. EU database for high-risk systems

The EU database for high-risk AI systems is a key initiative under the Act, aimed at centralising and facilitating access to detailed information on these systems, thereby increasing transparency and strengthening regulatory oversight. This database will be set up and maintained by the European Commission in cooperation with the Member States and will contain detailed information on high-risk AI systems registered under the Act.

The obligation to register themselves and the high-risk AI system lies with:

- In the private sector, the provider or, where applicable, its authorised representative, and always before placing on the market or putting into service.
- In the public sector, deployers that are public authorities, agencies or bodies, or persons acting on their behalf, and always before putting into service or use.

In cases where AI is used for law enforcement, migration, asylum and border control management, registration will take place in a secure, non-public section of the EU database.

High-risk AI systems covered by point 2 of Annex III (AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity) will be registered at national level.

9.3.1. Functions and characteristics of the database: it must include specific data entered by both the system providers and the deployers, if they are public authorities. This data will range from details identifying the system and its providers to technical and compliance information. The European Commission is responsible for defining the technical specifications of the database and updating them with the assistance of a committee of experts.

9.3.2. Accessibility and privacy: the information recorded must be generally accessible to the public, ensuring that the database is easy to navigate and understand, although with specific restrictions for sensitive information that will only be accessible to market surveillance authorities and the Commission, unless there is express consent to widen access.

9.3.3. Data protection: it must only contain personal data to the extent necessary to fulfil its regulated functions, while maintaining compliance with EU data protection regulations. The management of the database will be carried out with a high level of security, including cybersecurity measures to protect the information stored.

This database represents a critical step towards greater transparency in the use of AI, allowing for more effective public and regulatory scrutiny of AI systems that may have a significant impact on security and fundamental rights.

10. Transparency obligations for providers and deployers of certain AI systems

The regulator has considered transparency on certain aspects of an AI system essential to meet the objectives of the Act, especially those classified as high-risk. The Act sets out clear requirements to be followed in order to promote transparency and public confidence in these advanced systems.

Providers must ensure that **any AI system intended to interact directly with individuals is clearly identified as such**, except where it would be obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect. This obligation aims to ensure that users are aware that they are interacting with an AI system, rather than a human being. This obligation extends to systems that generate synthetic content such as audio, image, video or text, which must be clearly marked to be recognisable as AI-generated.

In addition, deployers of specific systems, such as **emotion recognition or biometric categorisation systems**, must inform individuals exposed to these systems about its operation and the processing of their personal data.

Finally, **AI systems that manipulate images, audio or video content, especially those that create deepfakes**, should clearly disclose that this content has been artificially generated or manipulated.

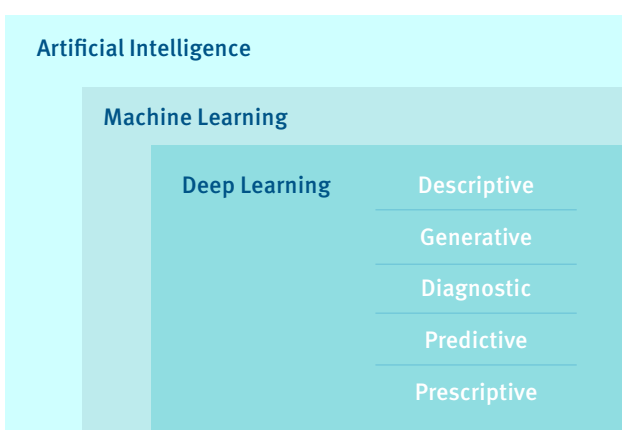
11. Use of AI by public authorities

Although it is a horizontal regulation, the Act pays particular attention to the use of AI systems by public bodies, because many of the uses of AI systems classified as high-risk are associated with typically administrative functions (AI systems in the administration of justice and democratic processes, migration, asylum and border control management, essential public services and benefits, etc.). Public bodies are therefore subject to the obligations associated with high-risk systems, both as providers (when they develop an AI system for their own use) and as deployers (when they contract the service to an external provider).

The Act specifies that public bodies using high-risk AI systems are required to carry out a fundamental rights impact assessment, the details and format of which will be developed by the Commission.

12. On general-purpose AI models

One of the most significant developments in the latest amendments to the Act is the establishment of a specific regulatory framework for general-purpose AI models, such as ChatGPT, Google Gemini and Meta Llama, which are designed to address a wide range of tasks and are often trained on large volumes of data using advanced methods such as self-supervised, unsupervised or reinforcement learning. These models can be marketed in a variety of ways, including as modules, libraries, direct downloads or physical copies, although the most common methods are via APIs or as a web service. These foundational models require additional components, such as user interfaces, to operate as functional AI systems.



Generative AI (GenAI) is one focus of AI research. It focuses on developing models capable of generating new and creative content, such as images, text or even music. Unlike traditional AI systems that rely on predefined rules or learned patterns, generative models are designed to produce original data by deeply understanding the underlying structures and characteristics of training data sets. These models fall into the category of machine learning, and use deep learning techniques to generate content similar to that created by humans. They rely on large language models (LLMs) to interact with users.

12.1. Classification

The Act distinguishes between general-purpose models and those that also present systemic risks.

A general-purpose AI model will be considered as a systemic risk model if it meets any of the following criteria:

- » It has high-impact capabilities, determined by appropriate technical tools and methodologies, including indicators and benchmarks.

- » According to a Commission decision, taken on its own initiative or in response to an alert from a panel of scientific experts, the model is recognised as having capabilities or an impact equivalent to those described in the previous point, taking into account the criteria specified in Annex XIII².
- » A general-purpose AI model will be assumed to have high-impact capabilities as described in the previous point, if the cumulative amount of computation used for its training, measured in FLOPs, exceeds 10^{25} ³.

In addition, the Commission is empowered under Article 97 to issue delegated acts to adjust the above-mentioned thresholds, as well as to update benchmarks and indicators in line with technological developments, such as improvements in algorithms or hardware efficiency.

These models must comply with specific obligations once they are placed on the market, including conducting impact assessments and stress tests to detect and mitigate potential risks.

Providers of these models should ensure high levels of transparency and cooperation with authorities, including detailed documentation on the model's design, capabilities and limitations. This information should be accessible not only to authorities but also to other providers integrating these models into broader AI systems.

12.2. Obligations

12.2.1. General purpose AI

The Act imposes a number of common obligations on providers of general-purpose AI models to ensure that these models are implemented in a responsible and safe manner. One of the main obligations is the production and continuous updating of the detailed technical documentation of the model. This documentation should include information on the training process, the tests performed and the results of the evaluations of these models. The specific elements to be covered are detailed in Annex XI of the Act and should be made available to the AI Office⁴ and national competent authorities on request.

In addition, providers must make this documentation available to other AI system providers who intend to integrate the general-purpose model into their own systems. This documentation should enable these third parties to fully understand the capabilities and limitations of the model and to comply with their own regulatory obligations. Importantly, this obligation extends without prejudice to the need to observe intellectual property rights and confidential business information.

Another significant obligation is to establish a policy to ensure compliance with Union law on intellectual property rights, particularly through the use of state-of-the-art technologies, to ensure the enforcement of these rights under the terms of Directive (EU) 2019/790, in particular in relation to text and data mining.

Providers must also draw up and make publicly available a detailed summary of the content used for the training of general-purpose AI models, according to a template provided by the AI Office.

In addition, providers of such technologies are expected to cooperate with the Commission and competent authorities in any regulatory action related to their models and to follow best practices and harmonised standards to demonstrate compliance with all these obligations.

12.2.2. General purpose AI with systemic risk

Providers of general-purpose AI models with systemic risk must comply with the following additional obligations: (i) perform model evaluation in accordance with standardised protocols and tools reflecting the state of the art, including conducting

2 For this purpose, Annex XIII sets out the criteria to be taken into account, such as: (i) The number of parameters of the model, which directly influences its complexity and processing power; (ii) The quality and size of the data set used to train the model, which can be measured by methods such as the use of tokens; (iii) The total amount of computation used to train the model, expressed in FLOPs or by combining other variables such as the estimated cost of training, the time required and the associated energy consumption; (iv) The input and output modalities of the model, including aspects such as text-to-text conversion in large language models, text-to-image conversion, multi-modality and the state of the art thresholds for determining high-impact capabilities for each modality, as well as the specific type of inputs and outputs, e.g. biological sequences; (v) Benchmarks and evaluations of capabilities of the model, considering aspects such as the number of tasks it can perform without additional training, its ability to adapt and learn new tasks, its degree of autonomy, scalability and the tools it has access to; (vi) The degree of impact it has on the internal market, especially if it has been used by at least 10,000 registered business users in the EU; (vii) The number of registered end-users interacting with the model.

3 FLOP or Floating Point Operations: any mathematical operation or task involving floating point numbers, which are a subset of the real numbers normally represented on computers by an integer of fixed precision raised by the integer exponent of a fixed base.

4 On 29 May 2024, the Commission announced the creation of the AI Office, established within the European Commission. The AI Office aims to enable the future development, implementation and use of AI in a way that fosters social and economic benefits and innovation, while mitigating risks, and will play a key role in the implementation of the Act, especially in relation to general-purpose AI models. The press release is available at the following link: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2982

and documenting adversarial testing of the model with a view to identifying and mitigating systemic risks; (ii) keep track of, document and report without undue delay any serious incidents together with potential corrective measures to the AI Office and, where appropriate, to the competent national authorities; (iii) ensure an adequate level of cybersecurity protection for both the AI model and its physical infrastructure, including measures to protect against malicious use or attacks that compromise the integrity and secure operation of the model; (iv) until a harmonised standard is published, providers may adhere to codes of practice to demonstrate compliance with these obligations (see section 12.3).

12.3. Codes of practice

Article 56 of the Act provides for the creation and promotion of codes of practice at EU level, which will be instrumental in ensuring that AI model providers adequately comply with the obligations imposed by the Act, and align their practices with the required ethical and legal standards. The AI Office will play a key role in encouraging and facilitating the development of these codes, ensuring that they cover the obligations specified in the previous articles, such as the proper documentation of models and systemic risk management.

The codes should include procedures and strategies to keep information up to date with market and technological developments, ensure an appropriate level of detail on the content used in model training, and define measures to assess and manage systemic risks. In addition, they should establish methods for documenting these risks and mitigating them, taking into account severity, likelihood and specific difficulties in dealing with them.

Once the Commission adopts a code of practice by means of an implementing act, it will gain general validity within the EU, i.e. providers adhering to an approved code will be presumed to be in compliance with the obligations of the Act. In the absence of a code of practice or if it is not considered adequate, providers must demonstrate compliance by other appropriate means, which must be approved by the Commission.

The codes of practice will include guidance on:

- | | | | | |
|---|---|--|--|--|
| <p>1.
Conducting societal impact assessments</p> | <p>2.
Implementing risk management systems</p> | <p>3.
Adopting risk mitigation measures</p> | <p>4.
Documenting and registering AI models</p> | <p>5.
Cooperating with the national competent authorities</p> |
|---|---|--|--|--|

The codes of practice are not binding in themselves, but serve as guidelines that AI system providers can follow to demonstrate compliance with the regulations set out in the Act. Adherence to these codes is voluntary, but once a provider chooses to follow a code of practice approved by the European Commission, it is presumed to comply with the obligations specified in the Act.

13. Measures to support innovation

As mentioned in the introduction, the European Union’s intention is for the Act to be a stimulus for AI innovation. To this end, this regulatory framework establishes a series of innovation support measures, including the following:

Regulatory sandboxes	The creation of controlled testing spaces to allow AI model providers to test their innovations in a controlled environment, under certain conditions and with the supervision of the authorities.
Advice and Support	Guidance and support from competent authorities to AI providers and developers on how to identify risks to the fundamental rights, safety and health of users, comply with regulatory requirements and expectations for responsible innovation.
Cooperation and coordinated work	Promotion of cooperation between competent national authorities, AI model providers and other stakeholders to share knowledge and experience.
Funding	Facilitating access to funding and support programmes for the research and development of AI models.

Standardisation	Promoting standardisation and certification of AI models to ensure safety and regulatory compliance.
SMEs	The inclusion of specific measures that pay particular attention to small and medium-sized enterprises (SMEs), including start-ups.

13.1. AI regulatory sandboxes

Regulatory sandboxes are safe and regulated environments in which companies, researchers and developers can experiment with new AI products, services or systems without strict compliance with applicable regulations, but under a specific supervisory framework, for a limited period of time and ensuring that adequate safeguards are in place. Member States must ensure at least one national AI regulatory sandbox is established, which must be operational at the latest two years after the entry into force of the Act.

These spaces will be supervised by the competent national authorities and aim to:

- » **Encourage innovation:** provide an environment where innovation can take place with less risk and more freedom, which is especially useful for SMEs that may not have the resources to bear the costs associated with complying with complex regulations and thus facilitate the development and implementation of innovative AI models.
- » **Identify and mitigate risks:** identify and address potential security, privacy or ethical issues before products or services are released to the general market. The sandbox therefore enables providers to demonstrate the security and compliance of their AI systems, and facilitates the identification and addressing of potential risks and issues prior to full market introduction.
- » **Help regulators gain a better understanding of new technologies and their implications:** this could influence the creation of more effective policies and regulations adapted to the digital age.

13.2. Measures targeting providers and deployers of SMEs and start-ups

Article 62 of the Act sets out measures to support SMEs and start-ups, focusing on access to sandboxes, training and awareness-raising activities, communication and advice on the Act, and participation in standardisation. The measures envisaged by the regulator include the following:

- » Priority access to sandboxes is given to SMEs that have their registered office or a branch in an EU country, and meet certain conditions and selection criteria.
- » Specific awareness raising and training activities on the application of the Act will be carried out, tailored to the real needs of SMEs and start-ups.
- » Communication channels are foreseen, to be used for advice and to answer queries raised about the implementation of the Act.
- » The participation of SMEs in the standardisation development process will be encouraged.
- » Special considerations for conformity assessment fees are regulated depending on the size and market of SMEs.
- » The AI Office will be responsible for providing standardised templates, maintaining an information platform, organising communication campaigns and promoting the convergence in public procurement of AI systems.
- » In the event of non-compliance with certain provisions, SMEs may be subject to administrative fines, but the lower percentage or amount of the fine will apply, taking into account their economic capacity⁵.

⁵ See Article 99(6) of the Act.

13.3. Derogations for specific operators (microenterprises)

In response to criticism of the Act's over-regulation of start-ups, the European regulator has eased the bureaucratic burden for microenterprises⁶, which can simplify certain elements of the quality management system required by the Act (Article 17⁷), as long as they do not have partner or linked enterprises within the meaning the Recommendation. For its part, the Commission will develop guidelines to simplify these elements without compromising the level of protection or the requirements for high-risk AI systems. Such simplification will not exempt microenterprises from complying with other requirements and obligations under the Act, including those specified in Articles 9 to 15, 72 and 73.

14. Penalties

The Act establishes a system of fines in line with other recent European legislation, such as the General Data Protection Regulation ("GDPR"), the Digital Markets Directive and the Digital Services Directive, namely:

Up to EUR 35 million or up to 7% of the total worldwide turnover of the previous financial year (if this amount is higher)	in the event of non-compliance with the prohibition of the AI practices referred to in Article 5.
Up to EUR 15 million or up to 3% of the total worldwide turnover of the previous financial year (if this amount is higher)	for failure to comply with certain obligations ⁸ in relation to operators or notified bodies, other than those laid down in Article 5.
Up to EUR 7.5 million or up to 1% of the total worldwide turnover of the previous financial year (if this amount is higher)	for supplying inaccurate, incomplete or misleading information to notified bodies or national competent authorities.
Up to EUR 1.5 million	for Union institutions, bodies, offices and agencies in the event of non-compliance with the prohibition of the AI practices referred to in Article 5.
Up to EUR 750,000	for Union institutions, bodies, offices and agencies in the event of non-compliance with the requirements or obligations laid down in the Act, other than those provided for in Article 5.
Up to 3% of the total worldwide turnover of the previous financial year or EUR 15 million (whichever is higher)	for providers of general-purpose AI models found to have committed intentional or negligent infringements.

15. Entry into force and next steps

The Act is likely to be published in the Official Journal of the European Union in mid-July, will enter into force 20 days later and will be fully applicable after 24 months, with the following exceptions:

- Chapters I and II (practical prohibitions) will apply **six months** after the date of entry into force of the Act;

⁶ In accordance with the definition provided in the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, available at the following link: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32003H0361>

⁷ Providers of high-risk AI systems must establish a quality management system to comply with the Act. This system should document policies and procedures including compliance strategies, design, development, testing, technical specifications, data and risk management, post-market monitoring, incident reporting, and communication with authorities and stakeholders, adapted to the size of the organisation.

⁸ These obligations are: (i) those referred to in Article 16 for providers of high risk AI systems; (ii) the obligations of authorised representatives referred to in Article 22; (iii) the obligations of importers referred to in Article 23; (iv) the obligations of distributors under Article 24; (v) the obligations of deployers under Article 26; (vi) the requirements and obligations of notified bodies under Articles 31, 33(1), 33(3) and 33(4) or Article 34; (vii) the transparency obligations of providers and users under Article 50.

- Codes of practice must be finalised **nine months** after the date of entry into force of the Act;
- Chapter III Section 4, Chapter V, Chapter VII and Chapter XII (obligations for the governance of general-purpose AI) will apply **12 months** after the date of entry into force of the Act, with the exception of Article 101;
- Article 6(1) and the obligations for high-risk systems will apply **36 months** after the date of entry into force of the Act.

RELEVANT MILESTONES

Entry into force: 20 days after its publication in the OJEU.

- **Three months later:** Communication of national authorities and national development of the penalties regime.
- **Six months later:** Prohibition of unacceptably risky AI.
- **Nine months later:** The codes of practice must be ready.
- **12 months later:** Applicability to general purpose AI.
- **18 months later:** Publication of practical implementation guidelines.
- **Two years later:**
 - Date of general application.
 - The Commission will need to assess and report on the need to amend the list of high-risk areas and every four years thereafter.
- **At five years:** Revision of the Act.

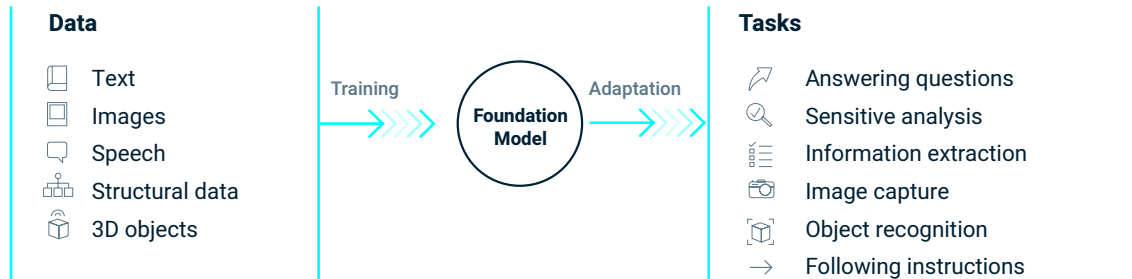
16. Key challenges for companies posed by the Act

The regulation of AI presents significant challenges that are at the heart of contemporary discussions on technology and regulatory policy. With the Act, European legislators have opted for early regulation, trying to anticipate possible abusive uses of AI or types of innovation that they consider detrimental to society. However, regulation itself can be a challenge for innovative companies because of the limits and restrictions it imposes on them, on a theoretical level, in order to balance the promotion of technological development with the responsible and ethical use of technology. Some of the challenges companies will face in the coming years include the following:

- **Business adaptation:** the Act is extensive and may be open to a wide range of interpretations. Companies developing and using AI systems will have to comply, often without knowing exactly how to interpret and implement the obligations of the Act. Understanding the interaction between the Act and existing rules applicable to AI, including on data protection, intellectual property and data governance, will also be a key issue for organisations. Failing to properly manage these interactions can be a significant source of risk for organisations. Therefore, it is not only a question of legal compliance. The Act will affect the way organisations invest in innovation, which will directly impact business.
- **Brussels effect:** the European regulator has repeated the so-called *Brussels effect* of the GDPR in the Act. This is intended to impose the obligations and principles of the Act on all regulated entities, irrespective of their country of origin, whenever they market their products or services to the EU.
- **Technological evolution:** the rapid evolution of AI poses the challenge of keeping regulations up to date to address new developments, with a clear risk of obsolescence of the Act itself.
- **Implementation and enforcement:** Implementing the Act also poses challenges for authorities in terms of supervision and enforcement, requiring adequate resources such as training and monitoring tools.

17. What should companies do from now on?

More recent AI systems, in particular generative AI, which allows the development of text, video or synthetic images, are based on the transformer architecture, which is based on foundational models, referred to by the Act as “general-purpose AI models”. These models differ from AI systems in the latter’s autonomy and ability to influence physical or virtual environments, with general-purpose AI models exhibiting a considerable degree of generality and being able to competently perform a wide range of different tasks, regardless of how the model is placed on the market, and which can be integrated into a variety of downstream systems or applications.



In view of the great potential of general-purpose AI models, the European legislator has deemed it necessary to dedicate an entire chapter (Articles 51 to 56) to them, with specific obligations for providers (discussed in section 12.2), including the following:

- 1) Appoint an authorised representative who is established in the EU, if the provider is located in a third country;
- 2) Draw up and keep up-to-date technical documentation of the model, including its training and testing process and the results of its evaluation, which should be made available, upon request, to the AI Office and national competent authorities;
- 3) Draw up and keep up-to-date information and documentation to be made available to those who want to integrate the general-purpose AI model into their AI systems. Although the Act does not specify what information these providers must provide, it states that it should be sufficient to enable providers of AI systems to have a good understanding of the capabilities and limitations of the general-purpose AI model.
- 4) Put in place a policy to ensure compliance with intellectual property rights law, in particular with regard to the opt-out mechanism of Article 4(3) of Directive (EU) 2019/790.
- 5) Make publicly available information on the content used to train the general-purpose AI model, following the format provided by the AI Office.
- 6) In the event of a general-purpose AI model with systemic risk, due to its high impact, the following additional requirements must be met:
 - a) Notify the European Commission without delay as soon as it is known that this requirement will be met;
 - b) Evaluate the model, including conducting and documenting adversarial simulation tests to identify and mitigate systemic risk;
 - c) Keep track of and, where appropriate, report serious incidents and possible corrective measures; and
 - d) Ensure an adequate level of cybersecurity protection.

These obligations should only be respected by general-purpose AI models. This selective approach underscores the importance of the recent adoption of the Act, which marks a milestone in the regulation of this emerging technology, and will affect, in one way or another, any company using an AI system. This new legal context imposes significant challenges, but also opportunities, which in order to be taken advantage of will require a thorough understanding of the new regulations and how they can affect organisations and individuals.

In the following pages, we present a series of recommended practical actions to successfully navigate this new regulatory landscape, ensuring that the implementation and use of AI is conducted in an ethical, safe and legally compliant manner.

From the perspective of implementers or professional users, we propose the adoption of the following measures:

- **Assess the impact of the Act:** we believe it is essential to assess the impact of the Act as soon as possible to understand how it will affect the organisation and its operations. It is very likely that the life cycle of AI technologies to be implemented or developed after the entry into force of the Act will be longer in the next two years (effective date of implementation in most cases); waiting until then could put investments at risk and damage the organisation's reputation.
- **Identify affected areas of the organisation and design a governance model:** it will be necessary to determine which internal actors will be affected by the implementation of AI systems and how. This will enable the design of a governance model that will help to ensure coordinated and consistent action in this area, balancing compliance aspects with the business approach.
- **Develop a training plan:** Focusing on training and awareness-raising at an early stage will help to improve the interpretation of the impact of the Act in the different areas and achieve the best possible outcome from the new context. Training should focus not only on the purely formal compliance aspects but also on the ethical and reputational perspective, as well as on the responsible and efficient use of this technology, thus helping to minimise risks in a broad sense. An initial shock plan is necessary, but it is also necessary to design and implement a continuous training plan that allows the organisation to keep up to date with foreseeable business, technological and legal changes, while at the same time maintaining the necessary standards of knowledge and awareness over time.
- **Legal by design:** the new legal framework will need to be integrated into innovation processes from the outset to ensure compliance from the design of AI systems. Moreover, the Act is one of many pieces of legislation with an impact on the digital domain. Designing a data model that is sufficiently adaptable to regulatory changes and that allows for the implementation of different layers of compliance will help to improve the efficiency of the organisation's processes and systems.
- **Make an inventory of AI-based solutions:** making an inventory of all AI-based solutions used by the organisation and classifying their level of risk is not only a requirement for legal compliance, but a strategic tool that will enable organisations to manage risk, optimise resources, and remain agile and accountable in a complex and constantly evolving technology landscape.
- **Prepare specific AI policies:** these policies should cover various aspects of the AI lifecycle and use, ensuring that all related activities are conducted in an ethical, safe and legally compliant manner (use, development, procurement, data protection, audit and compliance).
- **Map risks and assess acceptable thresholds:** this process involves identifying, analysing and prioritising the risks associated with the use and development of AI, as well as setting clear limits on what is considered an acceptable level of risk. This proactive approach to risk management will be essential to build trust and ensure long-term success in the use of AI technologies.
- **Adapt procurement processes with AI providers:** contractual models will need to be adapted to ensure that AI providers comply with the Act, update approval processes and develop third party risk management mechanisms in this area. Some of the key actions in this area will be: the definition of specific requirements, evaluation procedures, negotiation criteria, the management of intangible rights, and the training of procurement areas and contract negotiators.
- **Review and update insurance policies in relation to the use and development of AI systems:** the first step will be to conduct a detailed assessment of the risks associated with the use and development of AI systems. This includes technical risks, such as software failures or security breaches, as well as legal and ethical risks, such as privacy violations or liability for automated decisions. Based on the risk assessment, existing insurance coverage should be reviewed to identify possible gaps or exclusions that could leave the organisation exposed to AI-related risks. From there, work should be done with insurers to develop or adjust policies that specifically address the risks associated with AI. This may include cover for errors and omissions in software development, product liability, data breaches and other technology-specific risks.
- **Assess the impact on fundamental rights:** AI has the potential to significantly influence several fundamental rights, including privacy, non-discrimination, freedom of expression, and the right to fair assessment and decision-making. Just as the GDPR requires a DPIA (Data Protection Impact Assessment) to be carried out in some cases, organisations will have to develop FRIA (Fundamental Rights Impact Assessment) models under the Act.
- **Adapt the organisation to all the requirements of the Act:** taking into account the deadlines set by the Act, it will be necessary to develop and implement a comprehensive compliance plan. Some measures depend on implementing acts that will be undertaken by public administrations over the next two years and will therefore not be executable from the outset.

Pérez-Llorca

TECHLAW

Artificial intelligence

JUNE 2024

A challenge for companies and for regulators

Barcelona

-

Brussels

-

Lisbon

-

London

-

Madrid

-

New York

-

Singapore

perezllorca.com

However, it is key to design a strategy in this respect and to coordinate the adaptation timetable with the set of technological and business decisions that the organisation plans to develop in this area.

- **Analyse data used to train general-purpose AI models:** given the transparency obligations set out in the Act regarding data sets used to train a large-scale language model or foundational model, companies using AI systems, especially generative AI, should ensure that they have been trained with data that does not infringe third party rights and is sufficient to meet obligations with respect to the fundamental rights of citizens. Such analysis must be duly documented to be shown to the AI Office if required.
- **Develop mechanisms for the protection of intangible assets:** this aspect is particularly significant both in terms of the internal development of AI systems and in terms of the acquisition of third-party solutions, including hybrid scenarios and those involving free software or open licences. In many cases, the protection of intangible assets can only be achieved by relying on trade secret protection legislation. This legislation is particularly rigorous when it comes to assessing the protection mechanisms implemented from the earliest stages of conceptualisation of the solution to be protected. It is also key to assess the steps that will be taken to avoid infringements of third party rights in processes such as training AI tools or fine tuning, among others.
- **Monitor legal and regulatory developments:** keep up to date on legal and regulatory developments to adapt to any changes in AI legislation.
- **Participate in the design of good practices:** we recommend participating sectorally in the design of good practices in order to share knowledge and experiences with other organisations. The Act is a very cross-cutting regulation and it is full of concepts that are open to interpretation. Verticalisation by sectors of activity, specific use cases or technologies through the definition of legal-technical standards and good practices can help to increase the degree of legal certainty in this area, facilitating investment and support for innovation, while maintaining the necessary balance with the safeguards required by the Act.
- **Develop a tailored audit model and plan:** this approach will allow for effective assessment of the compliance of AI systems with applicable regulations, ethical standards and security requirements. By adopting a systematic and evidence-based approach, organisations will be able to demonstrate their commitment to accountability and excellence in AI implementation.

These are just some of the actions that companies using AI systems can take today to ensure a smooth transition to compliance with the Act, with a positive and enabling perception of this new technology, which we have no doubt will bring about significant changes in society and business.