AI ACT — KEY POINTS

MARCH 2024

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

After almost three years of the European Commission's proposal, the Artificial Intelligence Regulation (AI Act) has been given its final shape. Voting at committee level took place on 13 February and all that remains is for the final text to be approved by the plenary of the European Parliament, which, having previously been expected for mid-April, is now scheduled for March 13.

Having in mind that the text recently approved by key committees is already very close to its final version, Morais Leitão's Digital Cluster – Artificial Intelligence team hereby presents a brief guide to the key points of the AI Act.

I. GENERAL NOTES: CONTEXT, SCOPE AND DEFINITIONS

AI Act is designed to protect the internal market and to establish a uniform legal framework for AI systems, in conformity with European Union (EU) values. The AI Act brings relevant new definitions and is applicable to multiple operators of AI systems.

WHAT WERE THE ORIGINS OF THE AI ACT?

Since the European Commission adopted the proposal for the AI Act on 21 April 2021, the European institutions and Member States have been discussing how to deal with artificial intelligence within an EU framework, ensuring both free movement of AI-based goods and services and the protection of fundamental rights.

To prevent different national rules and restrictions, which would lead to the fragmentation of the internal market and thus decrease legal certainty for operators, the AI Act enshrines a consistent and high level of protection throughout the EU to achieve trustworthy Artificial Intelligence (AI) systems..

The AI Act comprises several purposes: *(i)* to improve the functioning of the internal market by laying down a uniform legal framework for AI systems, in conformity with EU values; *(ii)* to promote the uptake of human centric and trustworthy AI while ensuring a high level of protection of health, safety, fundamental rights (including democracy and rule of law) and environmental protection; and *(iii)* to support innovation.

TO WHOM WILL THE AI ACT BE APPLICABLE?

The AI Act shall apply to multiple operators of AI systems:

- *(i)* providers placing AI systems on the market or putting them into service within the Union, irrespective of whether they are established/located in the EU or in a third country;
- *(ii)* deployers established/located in the EU;
- *(iii)* providers and deployers established/located outside the EU when the output produced by their system is used within the Union;
- *(iv)* importers and distributors;
- *(v)* product manufacturers;
- *(vi)* authorised representatives of providers outside the EU; and
  (vii) affected persons located in the EU.

Matters of national security and models for the sole purpose of scientific research and development are explicitly excluded from the AI Act.

WHAT ARE ITS MAIN DEFINITIONS?

The definition of an AI system, as it currently stands, – "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" – was updated towards becoming more closely aligned with the ongoing work of international organisations working on artificial intelligence (*e.g.*, OECD). Also, this definition is not intended to cover simpler traditional software systems or programming approaches, which are based on the rules defined solely by natural persons to automatically execute operations.

Other relevant definitions include the distinction between "provider" (who develops an AI system and places it on the market or puts the system into service), "deployer" (who uses the AI system), "importer" (who places on the EU market an AI system from a person outside the EU) and "*distributor*" (who makes an AI system available in the EU and is not a provider or importer).

II. PROHIBITED AI PRACTICES

Several AI practices are prohibited by the AI Act, albeit with the possibility of exceptions in which provisions are established in order to mitigate the possible risks. The prohibition of certain practices aims to guarantee a minimum level of protection for fundamental rights.

WHAT AI MECHANISMS ARE PROHIBITED?

According to Article 5, the placing on the market, putting into service or mere use of AI systems that, with the objective of distorting or modifying behavior, in a way that causes or is likely to cause significant harm to a person or a group is prohibited when it:

- Uses purposefully manipulative or deceptive techniques or;
- Exploits personal vulnerabilities,[1] as well as the use of biometric categorization systems that categorize people based on their biometric data to deduce their other characteristics.

Systems that lead to the evaluation or classification of people based on their behavior, inferring personal characteristics from it, leading to unfavorable treatment in contexts other than those for which the data was collected or merely unjustified or disproportionate, are prohibited.

Regarding law enforcement, and with regard to biometric data, systems that allow remote "real time" identification and in public places are prohibited, except insofar as their use is strictly necessary for:

- The search for victims of crimes such as abduction, human trafficking and sexual exploitation, as well as search for missing persons;
- The prevention of a specific, substantial and imminent threat to people's lives or safety, or a genuine and present (or foreseeable) threat of terrorist attack;
- Locating or identifying a person suspected of committing a crime for the purposes of criminal investigation or execution of sentence, when the crime is punishable by a custodial sentence or a detention order for a maximum period of at least four years.

In addition, predictive policing mechanisms are prohibited when they are based on predicting the risk of committing a crime, based on profiling an individual. However, systems that assess a person's involvement in criminal activity are not prohibited when they are based on objective and verifiable facts.

Finally, systems that create or expand facial recognition databases by collecting facial images on the internet or CCTV and those that deduce emotions in workplaces and educational establishments are banned, except when health or safety reasons are involved.

WHAT ARE THE CIRCUMSTANCES IN WHICH EXCEPTIONS TO THE BAN APPLY?

The exceptions to the ban on the use of "real-time" remote biometric identification systems in places accessible to the public are not immediately applicable and the conditions for their application are clearly defined. In each case, a judgment must be made based on the public interest, a balance between the potential damage to be avoided (namely damage to the life and physical integrity of people) and the risks involved.

Although admissible, **such exceptions are not absolute and** must be circumscribed in time, space and the people to whom they apply, as well as subject to a prior impact assessment on fundamental rights, similar to high-risk AI systems, in order to identify specific risks for individuals or groups of individuals.

Its permitted use is subject to prior authorization, which will be binding, by a judicial authority or an independent administrative authority, especially with regard to the situations in paragraph 1(d) and paragraph 2 of this article. This requires the submission of a reasoned request, in line with the rules of national law expressed in paragraph 4 of this article, accompanied by clear and objective evidence that the use of the system in these ways is necessary and proportionate to the pursuit of one of the objectives specified in paragraph 1(d), limited to what is absolutely essential (in terms of time and

1. This prohibition does not apply to the labelling or filtering of legally acquired biometric data sets, such as images, on the basis of biometric data, nor to the categorization of biometric data in the criminal field.

geographical and personal scope). Authorities shall ensure that no decision is binding where it is taken solely on the basis of the results of the remote biometric identification system.

For these authorizations, member states are required to comply, as a minimum (because they are allowed to establish more restrictive rules), with the conditions listed in Article 5(1)(d), (2) and (3), as well as to lay down, in detail, in their national legislation, the objectives that may justify the use of these systems and the rules associated both with the procedure for requesting, issuing and exercising this authorization, as well as the control of these and the presentation of the associated report.

Once notified of these uses, the national authorities of the member states must submit an annual report to the Commission, which will follow the model provided by the Commission. These reports will be published annually by the Commission, excluding sensitive data relating to the activity of police authorities.

CAN THESE EXCEPTIONS BE APPLIED AS A MATTER OF URGENCY, WITHOUT AN IMPACT ASSESSMENT ON FUNDAMENTAL RIGHTS?

In situations where justified urgency makes such request impossible, the use of the system may be initiated without prior authorization. However, this must be justified promptly, within a maximum of 24 hours, and an impact assessment on fundamental rights must be submitted, where possible.

If this authorization is rejected, the use of the system in question will cease immediately, leading to the deletion of the data and all results and products obtained from this use.

CAN MEMBER STATES LEGISLATE ON THESE EXCEPTIONS?

The proposal for a Regulation allows states to impose more restrictive regimes and also requires them to lay down, in detail, in their national legislation, the objectives that may justify the use of these systems and the rules associated both with the procedure for requesting, issuing and exercising this authorization, as well as the monitoring of these and the presentation of the associated report.

WHAT ARE THE CONSEQUENCES OF THE PLACING ON THE MARKET, PUTTING INTO SERVICE OR MERE USE OF PROHIBITED AI SYSTEMS BY NATURAL OR LEGAL PERSONS?

The regulation sets fines for non-compliance at up to 35 million euros for individuals, or up to 7% of annual turnover for companies.

III. HIGH-RISK AI SYSTEMS

Between permitted and prohibited AI systems lie High-Risk Artificial Intelligence systems, outlined in Annex III of the Artificial Intelligence Regulation. Despite not being outrightly prohibited, these systems are subjected to specific limitations to mitigate potential risks.

WHICH ARTIFICIAL INTELLIGENCE SYSTEMS QUALIFY AS HIGH RISK?

High-risk AI systems represent the broadest category under the AI Act, in this sense they are mandated to comply with rigorous regulatory requirements in line with fundamental rights, health, and safety principles, aligning with the Charter of Fundamental Rights of the European Union.

In this context, the criteria for classifying AI systems as high-risk are based on their potential to harm health, safety, or fundamental rights. This assessment considers both the likelihood of such risks and the context of use.

An AI system is deemed high-risk if both of the following conditions are met:

- (i) the AI system is intended as a safety component of a product, or it is itself a product, which falls under the EU harmonization legislation listed in Annex II; and
- (ii) the product, for which the AI system is a safety component, or the AI system as a product, must undergo a third-party conformity assessment as per the EU harmonisation legislation in Annex II, for market placement or service provision.

In addition to fulfilling these requirements, if they are included in the list in Annex III, they will be considered High Risk in terms of their application to:

- Critical infrastructures (*e.g.*, public transportation), that could endanger citizens' safety;
- Educational or vocational training tools that might influence individuals' educational and career opportunities;
- Product safety components, like those in robot-assisted surgery;
- Employment and workforce management tools, including software used in hiring processes;
- Essential private and public services, such as credit scoring systems that can deny individuals loan access;
- Law enforcement tools that could affect fundamental rights;
- Migration, asylum, and border control management tools;
- Systems used in the administration of justice and democratic processes.

The AI Act further establishes that the provisions for high-risk AI systems will come into effect 36 months after the regulation's publication.

WHICH RULES ARE APPLICABLE TO PROVIDERS?

Pursuant to the AI Act, AI providers have a set of obligations in relation to High-risk AI.

Quality Management System: Providers of high-risk AI systems must implement a documented quality management system to ensure compliance with the AI Act. This system should cover various aspects, including *(i)* regulatory compliance strategies, *(ii)* design and development procedures, *(iii)* risk management, *(iv)* post-market monitoring, *(v)* incident reporting, *(vi)* data management, *(vii)* communication protocols, *(viii)* record-keeping, *(ix)* resource management, and *(x)* staff accountability.

The implementation of these requirements should be **proportionate to the size of the provider's organization** while ensuring the necessary level of rigor and protection. For providers subject to sector-specific Union laws on quality management systems, these requirements may be integrated into existing systems. Financial institutions subject to Union financial services legislation fulfill quality management obligations by adhering to internal governance rules, considering relevant harmonized standards.

In this regard, providers must comply with the following obligations:

Documentation Keeping: for a period of 10 years after the AI system is placed on the market or put into service. This includes technical documentation, quality management system documentation, records of approved changes by notified bodies, documents issued by notified bodies, and the EU declaration of conformity. Each Member State will establish conditions for retaining this documentation if the provider goes bankrupt or ceases activity;

Automatically generated logs: providers must maintain the automatically generated logs from their systems, as long as they are under their control, and for a minimum period of 6 months, unless specified otherwise by applicable Union or national law, especially regarding personal data protection;

Corrective Actions: providers must take immediate correction actions (*e.g.*, correction, removal, deactivation or recall) if they believe or have reason to believe that a system they have released onto the market or put into use does not meet the requirements of the AI Act;

Duty of Information: providers should notify the distributors of the system and, if applicable, the users, the authorized representative, and importers if a high-risk AI system poses a risk and the provider becomes aware of it. They must investigate the causes immediately, in cooperation with the deploying entity if relevant, and inform the market surveillance authorities in the Member States where the system was made available;

Cooperation with competent authorities: overall, providers must, *(i)* upon request by a competent authority, provide all necessary information and documentation to demonstrate compliance with the requirements, in a language understood by the authority in an official Union language determined by the Member State concerned, *(ii)* must grant access to system logs referred upon request by a national competent authority and, finally, *(iii)* the information obtained by a national competent authority must be treated confidentially;

Furthermore, the providers of high-risk AI systems established outside the Union must appoint an **authorized representative within the Union**. This representative shall perform the tasks specified in the mandate received from the provider. The authorized representative shall terminate the mandate if it considers that the provider acts contrary to its obligations under the AI Act, informing the relevant authorities accordingly.

Finally, providers and third parties supplying components or services for high-risk AI systems must specify information and assistance agreements. The AI Office may recommend model contractual terms for such agreements. These provisions must respect intellectual property rights and confidential business information.

HOW IS SUPERVENING QUALIFICATION AS A PROVIDER CARRIED OUT?

Any natural or legal person shall be considered a provider of a high-risk AI-system, subject to the respective obligations set out in the AI Act when they *(i)* place their own name or trademark on a high-risk AI-system previously placed on the market or put into service or *(ii)* substantially modify a high-risk AI-system already placed on the market or put into service or *(iii)* change the purpose of an AI-system (including GPAI systems) in such manner that the AI system becomes classified as high risk for the purposes of the AI Act.

In these cases, the former provider is no longer considered as a provider, although they shall cooperate and make available the information necessary for the fulfillment of the obligations relating to high-risk AI systems, except when the former provider has expressly excluded the change of its system into a high-risk system.

WHICH RULES ARE APPLICABLE TO DISTRIBUTORS?

Distributors must verify that high-risk AI systems *(i)* bear the required EC conformity marking, *(ii)* include the necessary documentation and instructions for use, that *(iii)* the supplier and importer have fulfilled their obligations, where applicable, and that *(iv)* storage and/or transport conditions do not compromise the AI system's conformity.

If there are grounds to believe that a high-risk AI system does not comply with the AI Act, the distributor must not make that system available on the market until it is brought into conformity.

Similarly, distributors must take all necessary corrective action, including withdrawal or recall from the market, if there are concerns or reasons to believe that a high-risk AI system placed on the market is not compliant. Distributors are responsible for ensuring that the provider, importer or any other operator involved takes the appropriate action.

In cases where a high-risk AI system poses a threat to health, safety, or fundamental rights, the distributor must inform the competent national authorities of the Member States where the product has been made available, as well as the provider or importer of that AI system, if applicable.

Finally, the AI Act outlines distributor duties to provide information and cooperate with competent national authorities upon receiving reasoned requests.

WHICH RULES ARE APPLICABLE TO IMPORTERS?

Before placing a high-risk AI system on the market, importers must ensure that the system *(i)* complies with the applicable rules; *(ii)* has all the necessary technical documentation; *(iii)* carries the European Certificate of Conformity (EC); and *(iv)* has an authorised representative appointed. The conditions for admissibility to the market must be ensured by importers when the system is under their responsibility, which includes storage and transportation.

Importers must also ensure that artificial intelligence systems which they believe do not comply with AI Act are not made available on the market, until all legal conditions have been met. Importers must also notify the supplier where the AI-system presents a risks to individuals' health, safety or fundamental rights.

When marketed, the AI system must also provide a set of indications, such as *(i)* the name of the importer, *(ii)* the registered trade name or trademark, and (*iii)* the respective contact address, information which must appear either on the packaging or in the accompanying documentation. Importers must keep a **copy of the certificate** issued by a competent authority, **instructions for use** and the **EU declaration of conformity**, where applicable, **for a period of 10 years** after the product has been placed on the market or put into service.

Importers must also cooperate with the competent authorities whenever requested, which, among other things, includes providing documentation in the language of the notifying authority.

WHICH RULES ARE APPLICABLE TO DEPLOYERS?

As part of the value chain of high-risk AI systems, the deployers are subject to a set of obligations based on a bipartite system.

The bipartition translates into the provision of:

1. "Universal" obligations, to which all deployers of high-risk AI systems are subject; and

2. Additional or specific obligations applicable only to certain deployers or in certain contexts or uses of high-risk AI systems.

The specificities that trigger the applicability of additional or specific obligations,[2] are connected with different elements, such as:

2.1. The nature of the deployer (*e.g.*, among others, deployers that are public authorities or deployers that are bodies governed by public law or private operators providing public services);

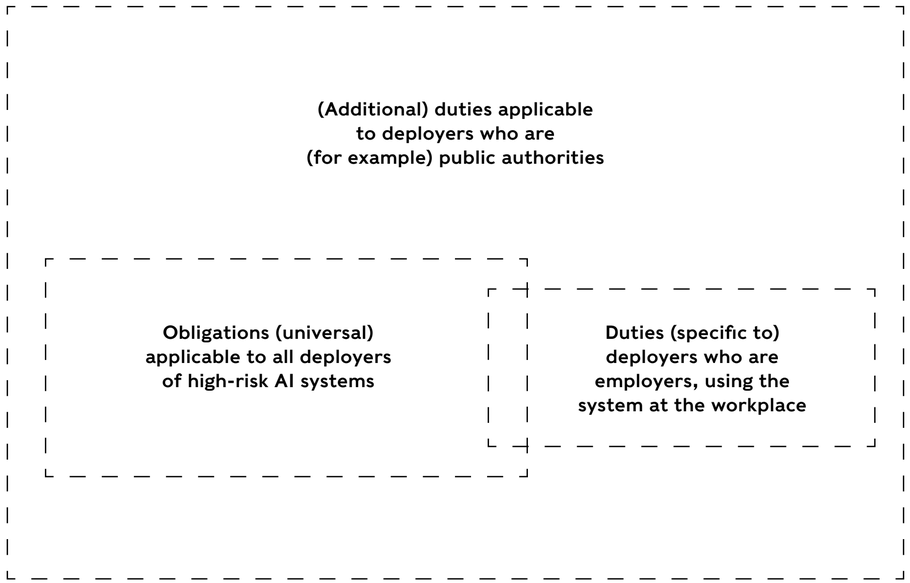
2.2. The quality under which the deployer acts and the context in which they use the system (*e.g.*, deployers who are employers putting into service or use a high-risk AI system at the workplace);

2.3. The purposes for which the deployer intends to use a high-risk AI system (*e.g.*, deployers using high-risk AI systems that make decisions or assist in making decisions related to natural persons); and also

2.4. The extent to which they may or may not have control over different aspects of the high-risk AI system used (*e.g.*, deployer exercising control over the input data of the high-risk AI systems they use).

2. Or its reconnection to the fulfilment of other governance duties arising from specific sectoral regulatory legislation, as is the case, of deployers who are credit institutions falling under Directive 2013/36/EU – Directive on the access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms – in which case the obligations set-out to monitor high-risk AI systems and to keep *logs* shall be deemed to be fulfilled by complying (or must be integrated in compliance) with the rules on internal governance arrangements or processes under Union financial services legislation that transposed such Directive.

A graphic example of part of what is explained above could be illustrated as follows:



Note that:

- The deployers subject to the additional duties are subject not only to such duties, but also to the "universal" obligations incumbent on all deployers of high-risk AI systems; and

- The same deployer may be subject to various types of additional or specific duties (*e.g.*, one same legal entity, in addition to the general obligations, may be subject to additional duties arising from its nature of public authority and, simultaneously, to the ones applicable to employers prior to using high-risk AI systems, at the workplace).

(Universal) obligations applicable (in all cases) to deployers of high-risk AI systems:

- Duty to take appropriate technical and organisational measures to ensure the use of the high-risk AI system in accordance with the instructions of use;

- Duty to monitor the operation of the high-risk AI system on the basis of the instructions of use and provide relevant data to the provider's post-market monitoring system;

- Duties to inform the provider of the high-risk AI system (or other stakeholders in the value chain) and to the relevant market surveillance authority when the deployer has reasons to consider that its use in accordance with the instructions of use may result in the AI system presenting a risk, insofar as risks to the health or safety or to fundamental rights of persons are concerned or if the deployer has identified any serious incident arising from the use of that system;

- Duties to suspend use of the system in such cases;

- Duty of the deployer to take into account (use) the information contained in the instructions of use to carry out a a data protection impact assessment (when required to carry out such assessment under the GDPR, whilst data controllers);

- General duties of co-operation with the relevant national competent authorities.

DEPENDING ON THE CONTROL OVER DIFFERENT ASPECTS OF THE SYSTEM USED, THE FOLLOWING OBLIGATIONS ARE ALSO FORESEEN:

- To the extent the exercises control over the high-risk AI system – Guarantee that the natural persons assigned to ensure human oversight of the high-risk AI Systems have the necessary competence, training, authority and support to ensure the oversight;

- To the extent the deployer exercises control over the input data – Ensure that the input data used in high-risk AI Systems is relevant and sufficiently representative in view of the intended purpose;

- To the extent the logs automatically generated by that high-risk AI system are under the control of the deployer – Keep *logs* automatically generated by the high-risk AI system for a for a period appropriate to the intended purpose (minimum of six months).

DEPENDING ON THE USE MADE OF THE HIGH-RISK AI SYSTEMS (IN CONJUNCTION, OR NOT, WITH A CERTAIN QUALITY OF THE DEPLOYER), THE FOLLOWING DUTIES SHOULD ALSO BE MENTIONED:

- Duty to inform the natural persons concerned of the use of high-risk AI systems for decision making affecting same natural persons;

- Duty (deployers who are employers) to inform workers representatives and the affected workers that they will be subject to the system, prior to putting into service or to using a high-risk AI system at the workplace;

- Duty to carry out a prior fundamental rights impact assessment for high-risk AI systems and to notify the market surveillance authority of the results of the assessment, for deployers who are a body governed by public law, who are a private operator providing public services or an operator deploying high-risk AI systems intended to be used to evaluate the creditworthiness or to establish credit scoring of natural persons or for risk assessment and pricing in relation to same persons in the case of life and health insurance, with some exceptions.

The Artificial Intelligence Office is expected to develop a template for a questionnaire, including through an automated tool to help deployers implement the prior fundamental rights impact assessment in a simplified manner.

Additional obligations applicable to deployers of high-risk AI systems applicable (exclusively) in view of the nature of the deployer:

- **Public authorities or Union institutions, bodies, offices and agencies (or persons acting on their behalf);**

- Self-registration, selection of the high-risk AI system and registration of its use in the EU Database on High-Risk Artificial Intelligence Systems;[3]

- Refrain from using the system if it is not registered in the aforementioned EU database and, in such case, inform the provider or the distributor.

There are also specific duties that provide additional safeguards regarding the **use of AI systems** (which are categorised as high-risk AI systems) on the use of post-remote **biometric identification**, particularly by **law enforcement authorities**.

3. See Articles 51 and 60 of the Regulation

IV. GENERAL PURPOSE AI MODELS

After several discussions since the publication of the first version of the AI Regulation by the European Commission, the institutions have reached an agreement on the regulation of general-purpose AI models, such as ChatGPT.

After several discussions occurred upon the launch of the first version of the AI Act proposal by the European Commission, the institutions reached an agreement on the regulation concerning general purpose AI models (**GPAI models**).

What is a GPAI?

GPAI models are defined as an AI model, including when trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable to competently perform a wide range of distinct tasks regardless of the way the model is placed on the EU market and that can be integrated into a variety of downstream systems or applications. A popular GPAI is ChatGPT.

What are the main obligations applicable to GPAI?

Transparency is a key word: when AI systems are intended to directly interact with natural persons, they shall be designed and developed in such a way that the concerned natural persons are informed or is clearly aware that they are interacting with an AI system.

Within the same rational, providers of AI systems generating synthetic data (audio, image or text) shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated content (unless it ruins the creative side of the work, like telling a joke about the interaction of AI systems with natural persons). For that, the concerned natural persons shall be informed in a clear and distinguishable manner at the latest at the time of the first interaction.

Regarding the tension between **copyright protection and text and data mining**, the AI Act makes it very clear that "*any use of copyright protected content requires the authorization of the rightholder concerned unless relevant copyright exceptions and limitations apply*". Where the rights have been expressly reserved by way of an "opt out" in an appropriate manner, providers of GPAI models will need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works. On this topic, the EU Act makes a very clear connection with Digital Single Market Directive.

Providers of GPAI models also must:

- Draw up and keep up-to-date the technical documentation of the model;
- Draw up, keep up-to-date and make available information and documentation to providers of AI systems who intend to integrate the general purpose AI model in their AI system;
- Put in place a policy to respect Union copyright law;
- Draw up and make publicly available a sufficiently detailed summary about the content used for training of the GPAI.

All GPAI have low or limited risk?

GPAI models qualify at least as limited risk AI. General purpose **AI models could, however, pose systemic risks** which include, but are not limited to, *(i)* any actual or reasonably foreseeable negative effects in relation to major accidents, *(ii)* disruptions of critical sectors and serious consequences to public health and safety, *(iii)* any actual or reasonably foreseeable negative effects on democratic processes, public and economic security or *(iv)* the dissemination of illegal, false, or discriminatory content.

Therefore, a GPAI model shall be classified as **GPAI with systemic risk** if it meets any of the following criteria:

a. It has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks – a general purpose AI model shall be presumed to have high impact capabilities when the cumulative amount of compute used for its training measured in floating point operations (FLOPs)[4] is greater than 10^25;

4. That is a measure of computational performance.

b. Based on a decision of the Commission.

In addition to the requirements set above, GPAI models with systemic risk must:

- Perform model evaluation with a view to identify and mitigate systemic risk;
- Assess and mitigate possible systemic risks;
- Keep track, document and report to the AI Office serious incidents;
- Ensure an adequate level of cybersecurity protection.

The Regulation encourages the compliance of the above referred obligations through the **adoption of codes of practice**.

It should be noted that irrespective of whether GPAI models are used as high-risk AI systems as such or as components of high-risk AI systems, GPAI models may be required to comply with the obligations set above.

Are these obligations applicable to all GPAI models?

For the benefit of innovation and growth opportunities in the EU ecosystem, **some of these obligations do not apply** should the provider offer the GPAI model under a **free and open source licence**,[5] except if such GPAI model poses systemic risks.

5. The licence should be considered free when users can freely access, use, modify and redistribute them or modified versions thereof.

V. MEASURES IN SUPPORT OF INNOVATION

Sandboxes will be set up at national level and real-world testing will be possible to allow businesses, in particular, SMEs and start-ups, to develop and train innovative AI systems before they are placed on the market.

HOW DO SANDBOXES WORK?

According to the AI Act, national competent authorities (alone or in cooperation with authorities of other Member States) shall establish at least one AI regulatory sandbox in physical, digital or hybrid form. An AI regulatory sandbox is defined as a concrete and controlled framework for (potential) providers of AI systems to develop, train, validate and test an AI system for a limited period of time and according to a sandbox plan describing the objectives, conditions, timeframe, methodology and requirements for the activities conducted within the sandbox.

AI regulatory sandboxes aim to foster innovation and accelerate market access, increase legal certainty, facilitate evidence-based regulatory learning, and support cooperation and sharing of best practices to the benefit of both companies and authorities. As an alternative to creating new sandboxes, existing ones may be used if such participation provides an equivalent level of national coverage. Under both options, the competent authority shall, at the request of the provider, provide written evidence of successfully completed activities and an exit report detailing both the activities and the related results and learning outcomes. These documents can and shall be used by market surveillance authorities and notified bodies to speed up conformity assessment procedures.

HOW DOES REAL-WORLD TESTING WORK?

In the context of AI regulatory sandboxes, which provide for a controlled environment for the development, training, testing, and validation of AI systems, **testing in real-world conditions may also be possible, subject to authorisation by national competent authorities**. This authorisation would be subject to specific terms and conditions, including safeguards to protect fundamental rights, health, and safety.

Furthermore, it is possible for providers or prospective providers of high-risk AI systems, as listed in Annex III, to conduct tests in real-world conditions outside of AI regulatory sandboxes. Such testing should adhere to a real-world testing plan, the elements of which will be detailed in implementing acts by the Commission.

Real-world testing **may occur at any stage** prior to the market introduction or implementation of the AI system, either independently or in collaboration.

To conduct real-world testing, providers (or prospective providers) must meet several conditions, including but not limited to:

1. Drafting and submitting a real-world testing plan to the market surveillance authority where the testing will take place;
2. Obtaining approval of the testing plan from the competent national authority;
3. Registering the real-world testing in the non-public section of the EU database, with a unique Union-wide identification number (with certain exceptions for high-risk AI systems in areas such as law enforcement, migration, asylum, and border control management);
4. Ensuring that the provider is established in the EU or has appointed a legal representative in the EU;
5. Implementing appropriate safeguards for data collected and processed for testing purposes;
6. Ensuring that individuals from vulnerable groups are adequately protected.

This framework not only enables market surveillance authorities to monitor these tests, but also enables providers to identify and mitigate incidents accordingly. Moreover, informed consent from testing participants is essential, meaning that providers must clearly communicate the nature, purpose and conditions of the test, and the participants' rights to withdraw consent.

ARE THERE SPECIAL PROVISIONS FOR SMES?

Small and medium-sized enterprises will benefit from a set of positive measures including **priority access** to test environments, dedicated communication channels and a **reduction of fees** that may be due following conformity assessments.

VI. GOVERNANCE AND ENFORCEMENT

The AI Act establishes a complex governance framework, with the coordinated intervention of new authorities responsible for the enforcement of the regulation at EU and national. Infringement of the AI Act could result in penalties that amount to large fines.

WHO WILL ENFORCE THE AI ACT IN THE EU?

The European Commission will establish the **AI Office** to develop EU expertise and capabilities in the field of AI and to contribute to the implementation of Union's AI legislation.

The AI Office will also monitor the deployment of AI systems and the obligations on providers (specially for high-risk systems and GPAI with systemic risk).

In addition to the EU AI Office, the AI Act also establishes the EU **AI Board** – composed of representatives of the Member States, a scientific panel of independent experts and an advisory forum – to advise and assist the Commission and the Member States to facilitate the consistent and effective application of the AI Act. The EU AI Board is responsible for a number of advisory tasks, including issuing opinions, recommendations, advice or contributing to guidance on matters related to the implementation of the AI Act, including on enforcement matters, technical specifications or existing standards regarding the requirements set out in the AI Act, and advising the Commission and the Member States and their national competent authorities on specific issues related to AI.

AND IN THE MEMBER STATES?

Member States shall establish at least two national competent authorities for the purposes of the AI Act: a notifying authority and a market surveillance authority.

These will be the national competent authorities that will exercise their powers independently, impartially and without bias to ensure the application and implementation of the AI Act in each Member State.

In particular, the AI Act requires the national competent authorities to have a sufficient number of permanently available staff whose skills and expertise include a thorough understanding of Artificial Intelligence technologies, data and data computing, personal data protection, cybersecurity, fundamental rights, health and safety risks and knowledge of existing standards and legal requirements.

Moreover, Member States should not create unjustified obstacles to the placing on the market or putting into service of high-risk AI systems that comply with the requirements set out in the AI Act.

In the case of criminal investigations, prior authorisation by judicial or administrative authorities is required for the use of AI systems for post-remote biometric identification.

MY COMPANY IS NOT HEADQUARTERED IN THE EU, DO I HAVE TO COMPLY WITH THE AI ACT?

Yes, if your company deploys or places on the market an AI system, whether you are established in the EU or in a third country, you must comply with the AI Act. Even if you train an AI system in a jurisdiction with lower copyright requirements, you must ensure a similar level of protection to that provided in the AI Act.

WHAT CAN HAPPEN IF THERE'S AN INFRINGEMENT?

Infringement of various aspects of the AI Act will result in penalties (fines) of **up to 35 million euros or up to 7% of a company's annual worldwide turnover** for the preceding financial year, whichever is higher.

However, there will be a **grace period** for providers of general purpose AI models and no fines can be imposed during the first year after the rules come into force.

What are the next steps of the AI Act?

- Publication: once formally adopted by the European Parliament and the Council, the AI Act will be published in the Official Journal of the EU;

- Entry into force: the Regulation will enter into force 20 days after publication;

- Transitional period: once published, the Regulation will then enter its transitional period, with most of the rules coming into force within 24 months.

CONTACT US

ARTIFICIAL INTELLIGENCE
ML Digital Cluster

Morais Leitão Digital Cluster – Artificial Intelligence will continue to closely monitor all developments concerning the Artificial Intelligence Regulation and remains at your disposal for any further clarification.

DIGITAL TOGETHER,
FIRM FOR TOMORROW.

HEAD OFFICE
LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTUGAL
ANGOLA
MOÇAMBIQUE
CABO VERDE
SINGAPURA

LexMundi
Member

mlgts.pt

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS