Assentian Limited

EU AI Act: Technical Conformity Guide

SECTION 01
SCOPE OF THE ACT

1. What is the territorial scope of the Act?

The Act has a broad territorial scope and is intended to have a wide application. It primarily places obligations on:

- Operators (defined below) of AI systems who are involved in offering an AI system (or the output of an AI system) to the EU market or who put an AI system into service within the EU; and
- Providers who place general purpose AI models on the market within the EU.

These obligations can apply even if the relevant Provider, Deployer or Distributor of an AI systems, or the relevant Provider of a general purpose AI model, are themselves located or established outside of the EU (Article 2).

2. What activities fall within the scope of the Act?

The Act imposes obligations for different categories of actor in the AI system production and deployment chain (collectively referred to as "Operators" in the Act). The type and extent of obligations which apply will depend on; (i) the category of Operator a person falls into; and (ii) the type and purpose of AI technology being used.

See table table to the right listing the different types of Operator covered by the Act.

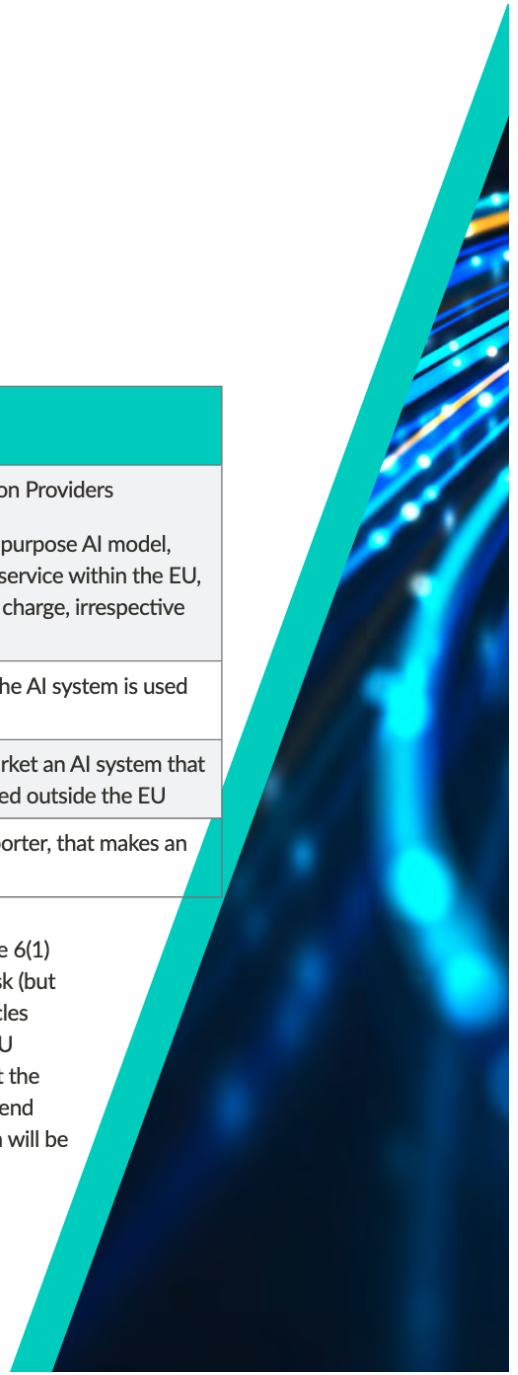
Exclusions from the scope of the Act

Article 2 of the Act specifically excludes certain uses of AI from the scope of the regulation. For example:

- the Act does not apply to the use of AI systems for military or national security purposes.
- the Act does not apply to the use of AI systems for the sole purpose of scientific research and development.
- the Act does not impose any obligations on Deployers who are natural persons using AI systems in the course of a purely personal non-professional activity.

Category of Operator	Description
Providers	The most significant regulatory burdens under the Act are placed on Providers Providers are any person that develops an AI system, or a general-purpose AI model, with a view to placing it on the market in the EU or putting it into service within the EU, under its own name or trademark, whether for payment or free of charge, irrespective of whether those providers are located within the EU
Deployers	Any person, using an AI system under its authority except where the AI system is used in the course of a personal, non-professional activity
Importers	Any person located or established in the EU that places on the market an AI system that bears the name or trademark of a natural or legal person established outside the EU
Distributors	Any person in the supply chain, other than the provider or the importer, that makes an AI system available on the EU market

Where an AI system is classified as "high risk" in accordance with Article 6(1) and (2) (discussed further below) and relates to the products which are covered by the EU harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 of the Act applies. Section B of Annex 1 contains a list of 8 pieces of product safety legislation, covering a range of products including aviation technology, agriculture and forestry vehicles, marine equipment, rail systems and motor vehicles. Article 6(1) identifies those systems as high risk (but does not impose obligations). Articles 102-109 amend certain existing EU legislation and Article 112 sets out the process for the Commission to amend the categories of AI systems which will be considered to be "high-risk".



3. What is considered an AI system under the Act?

An *"AI system"* is defined by Article 3 of the Act as:

- a machine-based system
- that is designed to operate with varying levels of autonomy
- that may exhibit adaptiveness after deployment
- 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. (Article 3(1))

This definition is intentionally broad and intended to cover a wide range of AI systems, including both complex generative AI tools and more basic systems utilising simpler techniques, like text matching, knowledge based responding, and decision trees.

AI systems that fall within this definition will include stand-alone AI software systems, systems integrated into a physical product (embedded), systems used to serve a physical product without being integrated into the product (non-embedded), or an AI component of a larger software system.

Under Article 96 of the Act the EU Commission must develop guidelines on the practical implementation of the Act. Article 96 identifies a number of specific elements which must, in particular, be the subject of such guidance and this includes the application of the definition of an AI system as set out in Article 3(1) - so there may be further development of this definition over time.

SECTION 02
CLASSIFICATION OF AI TECHNOLOGY AND OBLIGATIONS APPLICABLE FOR EACH CLASSIFICATION

How is AI technology classified under the Act

The Act identifies a number of different classifications of AI technologies, to which specific obligations will apply:

a. **Prohibited:** Certain AI practices are deemed to carry *'unacceptable risk'* and are therefore prohibited under the Act.

b. **High-Risk:** High-Risk AI (**HRAI**) systems used in the identified list of "high risk" contexts. Such systems are permitted but must comply with multiple requirements and undergo a conformity assessment before the system is released on the market.

   (Under the Act, the Commission will reassess the categorisation of Prohibited and HRAI systems annually and consider whether any amendments or adjustments are needed.)

c. **General Purpose AI Models:** the Act creates the classification of *"general purpose AI models"* (**GPAI Models**) and implements rules that apply to the development and use of such models.

d. **Transparency Obligations:** The Act also sets out certain transparency obligations which are applicable where AI systems are used for specific, narrow functions, regardless of the context (e.g. technology used for the production of "deep fake" images or audio).

   These "purpose-specific" rules are set out in Article 50 of the Act, so for ease of reference, we will term them as the ***"Article 50 Transparency Obligations"***. This should not be considered as a separate category of AI system, but rather an additional set of obligations which will apply to any AI system which can be used for the identified functions, regardless of whether it is a HRAI System, or a general purpose AI System, or neither.

We provide further detail on each classification below and summarise the different obligations that apply to each one under the Act.

A PROHIBITED AI SYSTEMS

The type of AI practices which are entirely prohibited under the Act are limited to a small number of use cases which have the potential to cause significant harm. They are AI systems that:

1. use **subliminal, deceptive or manipulative techniques** to materially distort the behaviour of a person or group or to impair their ability to make an informed decision (Article 5(1)(a))
2. **exploit vulnerabilities** (such as personality traits, social or economic situation, age, physical or mental ability) to materially distort a person's or a specific group's behaviour (Article 5(1)(b))
3. involve **social scoring evaluations**, based on social behaviour or personal characteristics, which lead to either (i) unfavourable treatment in contexts unrelated to the contexts in which the data was originally generated; or (ii) unfavourable treatment disproportionate to the relevant social behaviour (Article 5(1)(c))
4. predict or assess the likelihood of individuals **committing criminal offences**, based solely on the profiling of a natural person or on assessing their personality traits and characteristics (Article 5(1)(d))
5. create or expand **facial recognition databases through the untargeted scraping** of facial images from the internet or CCTV footage (Article 5(1)(e))
6. **infer emotions** of a natural person in the areas of workplace and education institutions, except where such use is intended for medical or safety reasons (Article 5(1)(f))
7. engage in **biometric categorisation** to categorise individual natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any filtering of lawfully acquired biometric datasets, such as images, based on categorising of biometric data in the area of law enforcement;(Article 5(1)(g))
8. use '**real-time' remote biometric identification** systems in publicly accessible spaces, unless such use is strictly necessary for (i) a search for abduction victims or missing persons; (ii) the prevention of an imminent or substantial threat to life or safety (e.g. a terrorist attack); or (iii) locating of a person suspected of criminal offence referred to in Annex II and punishable with a custodial sentence of at least 4 years (Article 5(1)(h))

There are some limited exceptions to some of these prohibitions, set out in Article 5 - for example, where the relevant AI systems are used for therapeutic medicinal purposes.

B HIGH-RISK AI SYSTEMS

Types of HRAI System

There are two general categories of AI system which will be considered "high-risk".

Category 1: The first category is:

- AI systems intended to form part of the safety component of a product, or
- the AI system is itself a product,

which is subject to the EU harmonisation legislation listed in Annex I of the Act, and the relevant product is required to undergo a safety assessment pursuant to that listed legislation. (Article 6(1)).

As noted above, pursuant to Article 2(2), where a HRAI system relates to products which are covered by the EU harmonisation legislation listed in Section B of Annex I, only Article 6(1), Articles 102 to 109 and Article 112 of the Act applies. Accordingly the legislation listed in Section A of Annex I is the key list in terms of the obligations which will arise under the Act.

Section A of Annex I lists 12 pieces of legislation covering a wide range of products including machinery, children's toys, recreational watercrafts, elevators, personal protective equipment, radio equipment, cableway installations, gas fuel appliances, diagnostic and medical devices.

Category 2: The second category is AI systems that operate in the areas identified in Annex III of the Act. In general these are use-cases which impact on critical areas of society or which have the potential to cause significant harm to the health, safety or fundamental rights of individuals.

The critical areas currently set out to **Annex III** are as follows:

No.	Critical area	Further details
1.	Biometrics	AI systems that are intended to be used for: ■ remote biometric identification ■ biometric categorisation according to sensitive or protected characteristics, based on the inference of those characteristics ■ emotion recognition systems. *"Biometric identification"* is the automated recognition of physical, physiological, and psychological human features for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a database (one-to-many identification). *"Biometric data"* is physical, physiological or behavioural characteristics which allow unique identification of a natural person - e.g. fingerprints, facial recognition, eye movement, body shape, voice, heart rate, blood pressure, keystrokes and emotional reactions. This category does not include AI systems used for biometric verification whose sole purpose is to confirm that a specific natural person is the person he or she claims to be.
2.	Critical infrastructure	AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic and the supply of water, gas, heating, and electricity.
3.	Education and vocational training	AI systems intended to be used to: ■ determine admission to educational and vocational training institutions ■ evaluate learning outcomes or assess the appropriate level of education for an individual ■ monitor and detect prohibited behaviour of students during exams
4.	Employment, workers management and access to self-employment	AI systems intended to be used: ■ for recruitment or employee selection, including for placing targeted job advertisements, screening or filtering applications and evaluating candidates ■ to make decisions affecting work related relationships, including, promotion and termination, task allocation, or for monitoring and evaluating performance.

The critical areas currently set out to Annex III *continued*

No.	Critical area	Further details
5.	Access to and enjoyment of essential private and public services and benefits	AI systems intended to be used: ▪ by public authorities to evaluate the eligibility of individuals for public assistance benefits and services, including healthcare services and essential services, such as housing, electricity, heating/cooling and internet, as well as to award, reduce or revoke such benefits ▪ to evaluate the creditworthiness of individuals with the exception of AI systems used for the purpose of detecting financial fraud ▪ to evaluate and classify emergency calls or to dispatch, emergency response services ▪ for risk assessment and pricing in relation to life and health insurance
6.	Law enforcement	AI systems intended to be used by law enforcement to: ▪ to assess the risk of a person becoming a victim of a criminal offence ▪ as polygraphs and similar tools ▪ to evaluate the reliability of evidence ▪ for profiling of individuals to assess the risk of offending or to profile individuals in the course of investigation of criminal offences
7.	Migration, asylum and border control management	AI systems intended to be used by public authorities ▪ as polygraphs and similar tools ▪ to assess a risk posed by an individual who intends to enter a Member State ▪ for the examination of applications for asylum, visa, residence permits and any complaints related to the eligibility of a person for migration status ▪ in the context of migration and border control management, for the purpose of detecting, recognising or identifying natural persons, with the exception of travel documents
8.	Administration of justice and democratic processes	AI systems intended to be used: ▪ by judicial authorities in researching and interpreting facts and the law and in applying the law ▪ for influencing the outcome of an election or referendum or the voting behaviour of individuals This does not include AI systems used to organise, optimise and structure political campaigns from an administrative and logistic point of view.

Exceptions and amendments

Where Providers of AI systems falling into one of the critical areas referred to in Annex III consider that their AI system does not pose a significant risk of harm to health, safety or fundamental rights, they must submit a reasoned notification to the national supervisory authority that they are not subject to the requirements applying to *"high risk"* systems (Article 6(3)). Such Providers will still be required to register that system with the EU Database, pursuant to Article 49.

Article 7 empowers the Commission to adopt delegated acts to amend Annex III by adding or modifying the listed areas or use-cases of HRAI systems.

Obligations of Operators in respect of HRAI systems

The obligations of each category of Operator in respect of HRAI Systems are summarised below:

Operator type: PROVIDERS

Obligations

The most onerous obligations in respect of HRAI Systems are placed on Providers. All HRAI systems must comply with a set of requirements set out in Chapter III, Section 2 of the Act (Articles 8-15). Some of these requirements are described in quite general terms but Article 8 provides some general guidance, stating that the expected compliance actions should take account of the intended purpose of the HRAI System as well as the existing state of the art. Providers are responsible for ensuring each of the requirements set out in Article 8-15; together with a number of additional obligations which are referenced in Article 16. It's helpful to provide a short summary of each obligation:

i. **Risk Management System (Article 9):** Providers must establish and document a risk management system in respect of the relevant AI system and ensure it is maintained throughout the lifecycle of the system, through updates and regular testing. The risk management system must involve:

- the identification and evaluation of reasonably foreseeable risks to health, safety or fundamental rights
- the evaluation of other possibly arising risks based on analysis of the data gathered from the post-market monitoring system required under Article 72
- the adoption of appropriate and targeted risk management measures to address the risks identified

ii. **Data and data governance (Article 10):** Where HRAI systems are developed using techniques that involve training of AI models with data, Providers must ensure that the data sets used for training, validation and testing comply with the requirements of Article 10. Article 10 sets out a number of broad data governance and management practices including:

- assessing the availability, quantity and suitability of the data sets that are needed for the identified purpose
- ensuring appropriate data-preparation measures, such as annotation, labelling, cleaning, updating, enrichment and aggregation
- identifying risks of potential biases which could impact on fundamental rights and appropriate measures to prevent such biases
- taking additional protective measures where data-sets involve special category data

Where HRAI systems are developed without using techniques involving the training of AI models, the data management requirements of Article 10 will still apply to the data sets used for testing.

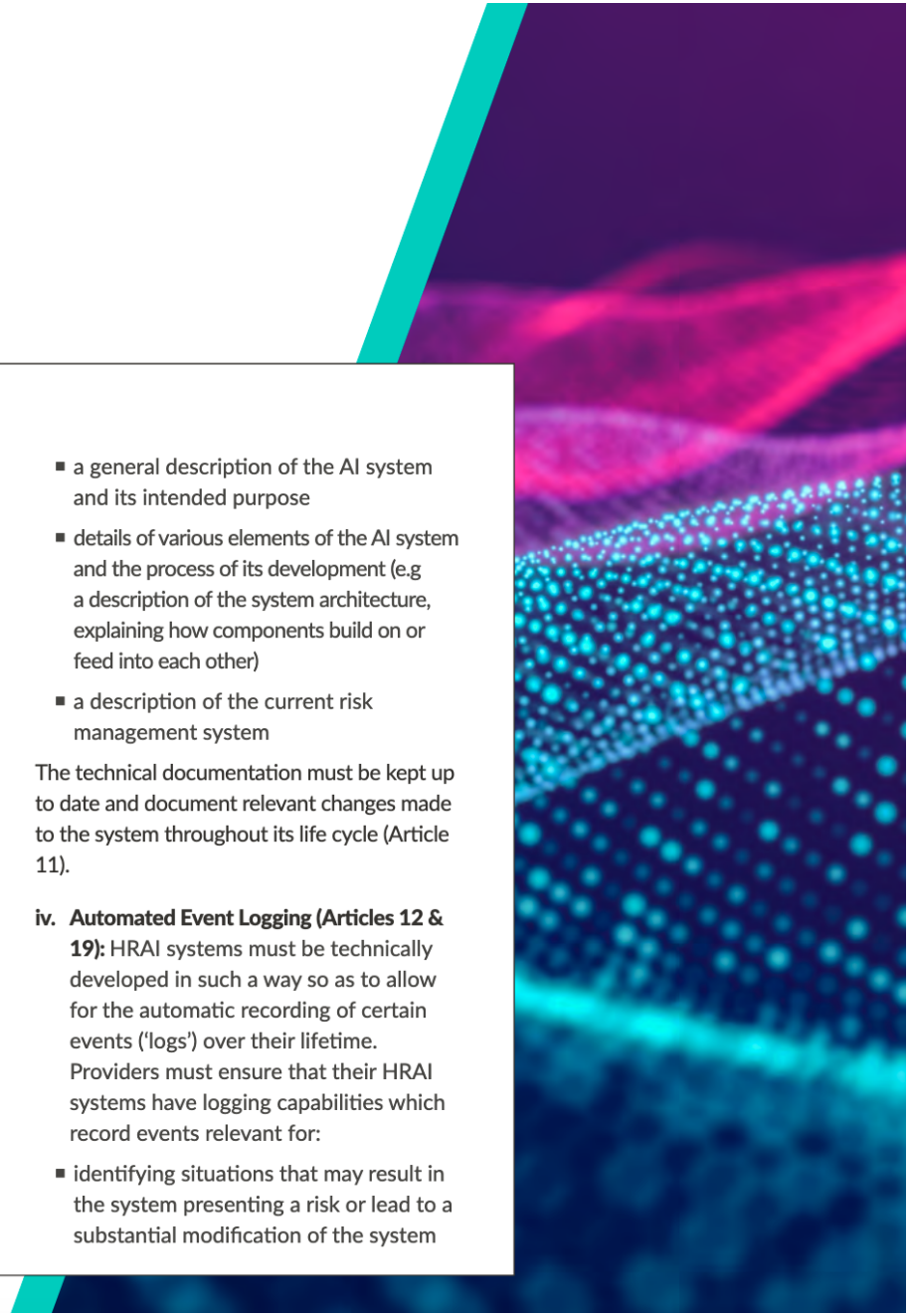
iii. **Technical Documentation (Article 11):** Providers must ensure that, before a HRAI system is placed on the market or put into service, appropriate technical documentation is prepared which sets out all of the elements described in Annex IV. This includes:

- a general description of the AI system and its intended purpose
- details of various elements of the AI system and the process of its development (e.g a description of the system architecture, explaining how components build on or feed into each other)
- a description of the current risk management system

The technical documentation must be kept up to date and document relevant changes made to the system throughout its life cycle (Article 11).

iv. **Automated Event Logging (Articles 12 & 19):** HRAI systems must be technically developed in such a way so as to allow for the automatic recording of certain events ('logs') over their lifetime. Providers must ensure that their HRAI systems have logging capabilities which record events relevant for:

- identifying situations that may result in the system presenting a risk or lead to a substantial modification of the system



Obligations of Operators in respect of HRAI systems

Operator type: PROVIDERS

- facilitating the post-market monitoring referred to in Article 72
- Deployers to monitor the operation of the system in accordance with Article 26
- Under Article 19, the automated logs discussed above must be kept for a period appropriate to the purpose of the HRAI system of at least 6 months unless otherwise provided under Union law.

v. **Provision of Information and Instructions to Deployers (Article 13):** Providers must ensure that HRAI systems are designed to ensure that their operation is sufficiently transparent to enable Deployers to understand a system's output and use it appropriately. HRAI systems must be accompanied by instructions for use that include concise, complete, and clear information that is relevant, accessible and comprehensible to deployers (Article 13). The instructions for use must contain:

- the identity and the contact details of the Provider and, where applicable, of its authorised representative
- information on the characteristics and capabilities of the system, including:
  - its intended purpose
  - the level of accuracy, robustness and cybersecurity against which the HRAI system has been tested and validated
  - any foreseeable circumstance, which may lead to risks referred to in Article 9(2) (Risk Management System)
  - where appropriate, any information that is relevant to explain and interpret its output
  - where appropriate, any information relevant to its performance regarding specific persons or groups of persons
  - where appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used
- any changes to the HRAI System which have been pre-determined by the Provider at the moment of the initial conformity assessment
- the human oversight measures referred to in Article 14
- the computational and hardware resources needed, the expected lifetime of the HRAI system and any necessary maintenance and care measures
- a description of the mechanisms included within the HRAI system that allows Deployers to store and interpret the logs in accordance with Article 12

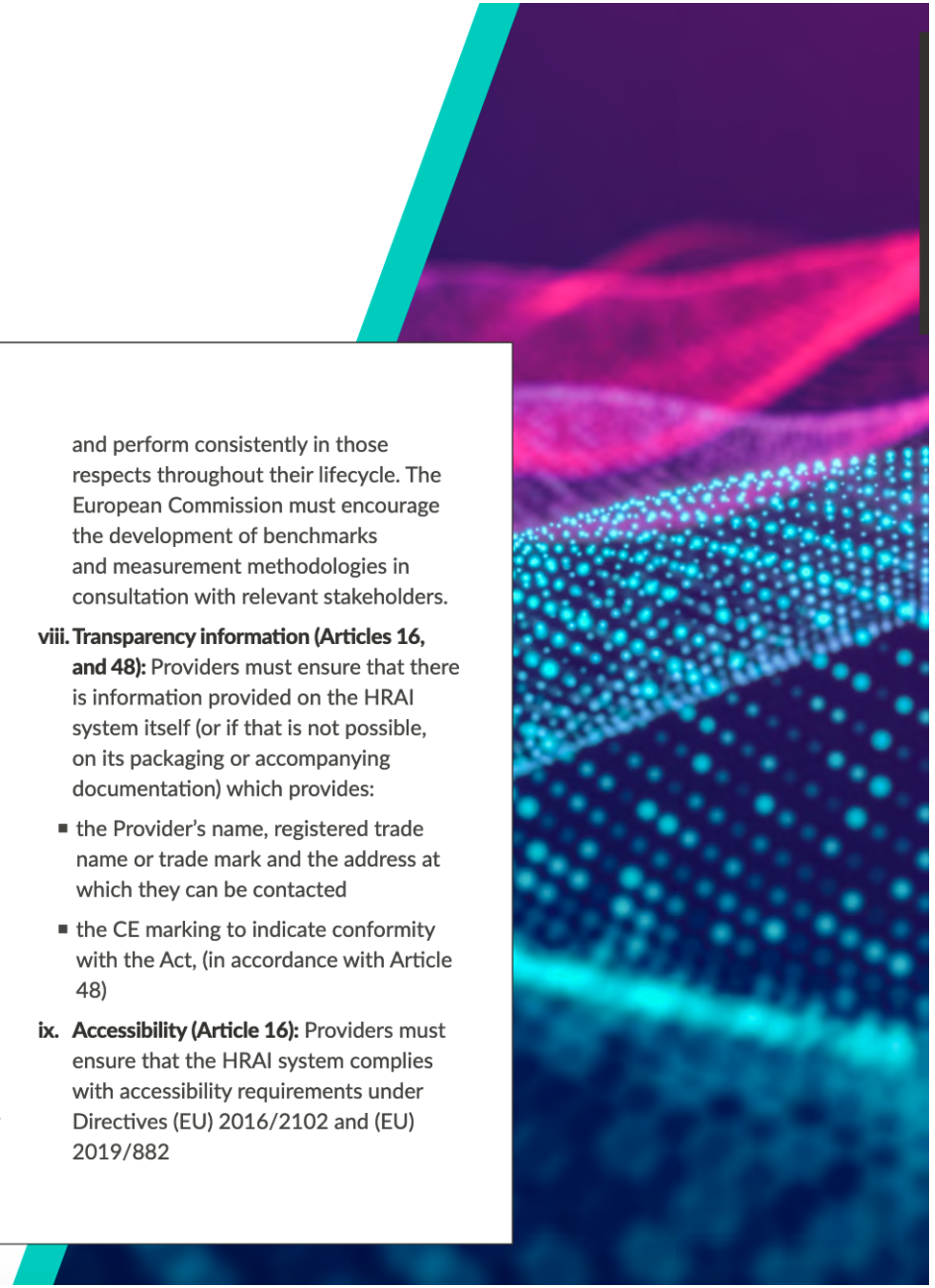
vi. **Human Oversight (Article 14):** Providers must ensure that HRAI are designed and developed in such a way so that they can be effectively overseen by natural persons during the period in which the AI system is in use. The level of oversight must be commensurate to the risks, level of autonomy and context of use of the AI system.

vii. **Accuracy, Robustness and Cybersecurity (Article 15):** Providers must ensure that HRAI systems are designed in such a way that they achieve an appropriate level of accuracy, robustness and cyber security and perform consistently in those respects throughout their lifecycle. The European Commission must encourage the development of benchmarks and measurement methodologies in consultation with relevant stakeholders.

viii. **Transparency information (Articles 16, and 48):** Providers must ensure that there is information provided on the HRAI system itself (or if that is not possible, on its packaging or accompanying documentation) which provides:

- the Provider's name, registered trade name or trade mark and the address at which they can be contacted
- the CE marking to indicate conformity with the Act, (in accordance with Article 48)

ix. **Accessibility (Article 16):** Providers must ensure that the HRAI system complies with accessibility requirements under Directives (EU) 2016/2102 and (EU) 2019/882



Obligations of Operators in respect of HRAI systems

Operator type: PROVIDERS

x. **Quality Management System (Article 17):** Providers must document and maintain a quality management system in the form of written policies, procedures and instructions that include a wide range of quality management measures including:

- a strategy for regulatory compliance
- techniques and processes to be used for design control and quality control
- the testing procedures to be carried out before, during and after the development of the HRAI system
- systems and procedures for data management
- the risk management system referred to in Article 9
- implementation of a post-market monitoring system in accordance with Article 72
- procedures for serious incident recording in accordance with Article 73
- an accountability framework setting out the responsibilities of management and other staff with regards to all details set out in the quality management processes.

xi. **Document Retention (Article 18):** For a period of 10 years after the HRAI system has been placed on the market or put into services, the Provider must keep a number of records ready and at the disposal of the national competent authorities. These includes:

- the technical documentation referred to in Article 11
- the documentation concerning the quality management system referred to in Article 17
- where applicable, the documentation concerning the changes approved or other decisions issued by notified bodies[1]
- the EU declaration of conformity referred to in Article 47

xii. **Corrective Actions, Duty to inform and *"Serious Incidents"* (Article 20 and Article 73):** Providers which have reason to consider that a HRAI system is not in conformity with the Act must immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate. They must also inform the other relevant Operators, as appropriate.

Under Article 20, where the HRAI Systems *"presents a risk"* and the Provider becomes aware of that risk, it shall immediately investigate the causes, and inform the Market Surveillance Authorities of the Member States in which the system is on the market and, where applicable, the relevant notified body, of the nature of the non-compliance and of any relevant corrective action taken.

The definition of an AI system which "presents a risk" is provided by Article 3 of the EU's Market Surveillance Regulation (2019/1020) and means any system which has the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security and other public interests, beyond what is considered reasonable in relation to its intended purpose.

Providers of HRAI Systems must immediately report any *"serious incidents"* or *"widespread infringements"* (as defined in the Act) to the Market Surveillance Authorities of the Member State where the incident occurred. A *"serious incident"* is one which leads to leads any of the following:

- death, or serious harm to a person's health
- a serious and irreversible disruption of the management or operation of critical infrastructure
- the infringement of obligations under Union law intended to protect fundamental rights
- serious harm to property or the environment

[1] *"Notified bodies" are discussed further below*

Obligations of Operators in respect of HRAI systems

Operator type: PROVIDERS

At a high level, a "widespread infringement" is an act or omission contrary to EU law which is likely to harm the collective interests of individuals residing in multiple Member States.

Article 73 provides the timelines for how soon a Provider (or as applicable, a Deployer), must notify a Market Surveillance Authority after becoming aware of the serious incident or widespread infringement. These reports must be made as soon as possible and depending on the type of incident, the maximum period for making a report can be as short as 2 days after the Provider (or Deployer) becomes aware of the incident. Article 73 also sets out the actions which a Provider and a Market Surveillance Authority should take subsequent to a serious incident being reported.

xiii. **Requests for information (Article 21):** Upon a reasoned request from a competent authority, Providers are obliged to provide relevant information to demonstrate conformity of the HRAI System with Articles 8-15 of the Act. Upon a reasoned request from a competent authority, Providers are obliged to provide access to the automatically generated logs of the HRAI system referred to in Article 12.

xiv. **Conformity Assessment and Declaration (Articles 43 & 47):** In accordance with Article 43, the Providers must complete an appropriate conformity assessment prior to being placed on the Market or put into service and subsequent to a substantial modification. Such a conformity assessment may give rise to knowledge of a risk associated with the system and engage the duty to take corrective actions and duty to inform, discussed at point (xii) above. The type of conformity assessment required will be dependent on the type of HRAI System at issue (see further detail in respect of conformity assessments in the *Guidance, Supervision and Enforcement Framework section* below).

Under Article 47, the Provider must also complete an EU declaration of conformity for each HRAI system they provide and keep it at the disposal of the national competent authorities for 10 years after the HRAI System has been placed on the market or put into service. The declaration of conformity must confirm the system's compliance with the Act and contain all of the information set out in Annex V. The declaration must be kept up-to-date as appropriate. Where HRAI systems are subject to other Union harmonisation legislation which also requires an EU declaration of conformity, a single EU declaration of conformity shall be drawn up in respect of all Union law applicable to the HRAI system.

xv. **Registration (Article 49):** Before placing on the market or putting it into service a HRAI System listed in Annex III (with the exception of systems referred to in point 2 of Annex III - *Critical Infrastructure*) the Provider must register themselves and their system in the EU database established under the Act.

Where an AI system falls into one of the critical areas referred to in Annex III, but the Provider has concluded that the system is not high-risk in accordance with Article 6(3), the Provider is still obliged to register that system in the EU database.

HRAI Systems referred to in point 2 of Annex III (Critical Infrastructure) shall be registered at national level.

xvi. **Post-marketing Monitoring (Article 72):** Providers must create a *"post-market monitoring system"* that is proportionate to the nature of the AI technologies and the risks of the relevant HRAI system. The *"post-market monitoring system"* must actively and systematically collect, document and analyse relevant data which allow the Provider to evaluate the continuous compliance of AI systems with the requirements set out in Article 8-15.

Obligations of Operators in respect of HRAI systems

Operator type: DEPLOYERS

Obligations

In general, deployers of HRAI systems are not expected to do the types of conformity verification required of Importers and Distributors. However the Act does impose high-level obligations to ensure Deployers operate an HRAI system in line with its instructions for use and requires Deployers to assist Providers in the Provider's continued monitoring of the system. The Act also identifies specific obligations for Deployers in respect of input data and providing certain information to natural persons who may be affected by the use of the system.

i. **General Operations (Article 26(1) and (2)):** Deployers of HRAI systems must take appropriate technical and organisational measures to ensure they use such systems in accordance with the instructions for use accompanying the system and that human oversight of the system to natural persons who have the necessary competence, training, authority and support

ii. **Input Data (Article 26(4)):** To the extent the Deployer exercises control over the input data, that Deployer must ensure that input data is relevant and sufficiently representative in view of the intended purpose of the HRAI system.

iii. **Post-market monitoring (Article 26(5) and Article 72):** Deployers must monitor the operation of the HRAI system on the basis of the instructions for use and, where relevant, provide information to Providers in accordance with Article 72, to allow Providers to properly monitor the system. Where deployers have reason to consider that the use of the HRAI system may present a risk they shall, without undue delay, inform the Provider or Distributor and the relevant Market Surveillance Authority, and shall suspend their use of that system. Where Deployers have identified a serious incident, they shall also immediately inform first the Provider, and then the Importer or Distributor and the relevant Market Surveillance Authorities of that incident.

iv. **Event Logging (Article 26(6)):** To the extent that the logs automatically generated by a HRAI system are under their control, Deployers must maintain such logs for an appropriate period given the intended purpose of the system, and not less than 6 months unless provided otherwise in applicable Union or national law

v. **Information for Employees (Article 26(7)):** Before putting into service or using a HRAI system at the workplace, Deployers who are employers must inform workers' representatives and the affected workers that they will be subject to the use of the HRAI system.

vi. **Registration Obligations for Public Authorities (Article 26(8) and Article 49):** Deployers of HRAI systems that are public authorities, or Union institutions, bodies, offices or agencies must register the intended use on the EU database, in accordance with Article 49(3). Where such Deployers find that the HRAI system that they intend to use has not been registered in the EU database referred to in Article 71, they may not use that system.

vii. **Data Protection Impact Assessments (Article 26(9)):** Where applicable, Deployers of HRAI systems shall use the information provided under Article 13 of the Act (i.e. the instructions for use) to comply with their obligation to carry out a data protection impact assessment under Article 35 of the GDPR.

viii. **Biometric Identification (Article 26(10)):** The Act sets out specific rules and authorisations required in respect of the use of an HRAI system by a Deployer to engage in biometric identification in the context of the targeted search of a person suspected or convicted of having committed a criminal offence:

ix. **Informing Subjects of Decisions (Article 26(11)):** Deployers of HRAI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons shall inform the natural persons that they are subject to the use of the HRAI system.

x. **Cooperation (Article 26(12)):** Deployers shall cooperate with the competent authorities in any action those authorities take in relation to the HRAI system in order to implement this Regulation.

xi. **Fundamental Rights Assessment for Use in Public Services (Article 27):** Deployers that are bodies governed by public law, or that are private entities providing public services, which intend to operate an AI system in any of the high risks contexts set out in Annex III of the Act - other than in the area listed in point 2 of Annex III (Critical Infrastructure) - must perform an assessment of the impact of fundamental rights that the use of such a system may produce.

Obligations of Operators in respect of HRAI systems

Operator type: IMPORTERS

Obligations

i. **Verifying conformity (Article 23(1))**: Before placing a HRAI system on the market, Importers must ensure that the system is in conformity with the Act by verifying that:
   - the relevant conformity assessment procedure referred to in Article 43 has been carried out;
   - the Provider has drawn up the technical documentation in accordance with Article 11;
   - the system bears the required CE marking and is accompanied by the EU declaration of conformity and instructions for use;
   - the Provider has appointed an authorised representative in accordance with Article 22(1).

ii. **Pre-Market Non-conformity and Risk Assessment (Article 23(2)):** Where an Importer has sufficient reason to consider that a HRAI system is not in conformity with the Act it shall not place the system on the market. Where the Importer considers that the HRAI system "presents a risk", the Importer shall inform the Provider of the system, the authorised representatives and the Market Surveillance Authorities to that effect.

iii. **Transparency Information (Article 23(3)):** Importers must indicate their name, registered trade name or trade mark, and the address at which they can be contacted in relation to the HRAI system on its packaging or its accompanying documentation.

iv. **Safety Measures (Article 23(4)):** Importers must ensure that, while a HRAI system is under their responsibility, the relevant storage or transport conditions, do not jeopardise the systems compliance with the requirements set out in Article 8-15.

v. **Document Retention (Article 23(5)):** For a period of 10 years after the HRAI system has been placed on the market or put into service, Importers must keep a copy of the instructions for use, the EU declaration of conformity and, where applicable the certificate issued by the notified body.

vi. **Requests for information (Article 23(6)):** Upon a reasoned request, Importers shall provide competent authorities, with all the necessary information and documentation, including that kept in accordance with Article 23(5), to demonstrate the conformity of a HRAI System with the requirements set out in Article 8-15.

vii. **Cooperation (Article 23(7)):** Importers must cooperate with competent authorities in any action those authorities take in relation to a HRAI system the Importers placed on the market, in particular to reduce and mitigate the risks posed by it.

Obligations of Operators in respect of HRAI systems

Operator type: DISTRIBUTORS

Obligations

i. **Verifying Conformity (Article 24(1)):** Before making a HRAI system available on the market, Distributors must verify that:
   - » The system bears the required CE marking,
   - » that it is accompanied by a copy of EU declaration of conformity and instructions for use;
   - » that the Provider and the Importer of the system, as applicable, have complied with their respective obligations to provide their information on the system or its packaging; and
   - » That the Provider as a quality management system in place.

ii. **Pre-Market Non-Conformity and Risk Assessment (Article 24(2)):** Where a Distributor has sufficient reason to consider that a HRAI system is not in conformity with the requirements in Article 8-15, it shall not place the system on the market. Where the Distributor considers that the HRAI system *"presents a risk"*, the Distributor shall inform the Provider or, as applicable, the Importer of the system to that effect.

iii. **Safety Measures (Article 23(3)):** Distributors must ensure that, while a HRAI system is under their responsibility, the relevant storage or transport conditions, do not jeopardise the systems compliance with the requirements set out in Article 8-15.

iv. **Post-Market Non-Conformity and Risk Assessment (Article 24(4)):** Where a Distributor has sufficient reason to consider that a HRAI system which it has placed on the market is not in conformity with the requirements in Article 8-15, it must make the corrective actions necessary to bring that system into conformity with those requirements, withdraw it, recall it, or ensure that any relevant Operator, as appropriate, takes those corrective actions.

v. **Requests for information (Article 24(5)):** Upon a reasoned request, Distributor shall provide competent authorities, with all the necessary information and documentation regarding its actions which is necessary to demonstrate the conformity of a HRAI System with the requirements set out in Article 8-15

vi. **Cooperation (Article 24(6)):** Distributor must cooperate with competent authorities in any action those authorities take in relation to a HRAI system the Distributor placed on the market, in particular to reduce and mitigate the risks posed by it.

As noted previously, Article 96 of the Act provides that the Commission must develop guidelines on the practical implementation of the Act and identifies a number of specific elements which must be the subject of such guidance. This list of specific topics includes the application of the requirements referred to in Articles 8 - 15 and in Article 25.

Provider Obligations applied to other Operators and Third Parties

Under Article 25 of the Act, any Distributor, Deployer or other third parties will be considered a Provider, and subject to all of the obligations of a Provider in respect of HRAI systems, if any of the following circumstances apply:

a. They put their name or trademark on a HRAI system which is already on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations therein are allocated otherwise

b. They make a substantial modification to a HRAI system that has already been placed on the market or put into service, where the system still remains a HRAI system pursuant to Article 6

c. They modify the intended purpose of an AI system, including a GPAI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a HRAI system in accordance with Article 6.

Where these circumstances occur, the Provider that initially placed the system on the market or put it into service shall no longer be considered to be a Provider of that specific AI system for the purposes of Act. The Provider may be obliged to cooperate with the new Providers, in order to assist them to comply with the Act, unless the original Provider has clearly specified that its AI system is not to be changed into a HRAI system.

Product Manufacturers

Under Article 25(3), in the case of HRAI systems that are safety components of products covered by the legislation listed in Section A of Annex I, the product manufacturer identified in that legislation shall be considered the Provider of the HRAI system, and shall be subject to the obligations under Article 16 under either of the following circumstances:

1. the HRAI system is placed on the market together with the product under the name or trademark of the product manufacturer
2. the HRAI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market

Authorised Representatives

Under Article 22, where a Provider of a HRAI system is established in a non-EU country, the Provider must appoint by written mandate, an authorised representative which is established in the EU. The Article specifies specific tasks which must be included in that mandate and which the Provider must enable its authorised representative to perform on its behalf.

Standards and Common Specifications

The Act makes a number of references to EU Regulation No 1025/2012 - also known as the *Standardisation Regulation*. The Standardisation Regulation provides a framework for certain *"European standardisation organisations"* to set out non-compulsory standards and standardisation deliverables for certain goods and services, in support of EU policies and EU law.

Article 40 of the Act provides that the Commission must, without undue delay, issue a request under Article 10 of the Standardisation Regulation to the European standardisation organisations for standards to be provided which cover all of the obligations under Article 8-15 and the obligations applicable to GPAI models (Articles 53-55).

Although such standards are not binding in nature, where a HRAI System is in conformity with a harmonised standard which has been published in accordance with the Standardisation Regulation, under Article 40 of the AI Act, the system shall be presumed to be in conformity with the requirements in Article 8-15 and/or Article 53-55, to the extent that such standards cover those requirements.

Under Article 41, where the Commission requests that standards be provided in accordance with Article 10 of the Standardisation Regulation but the standards either are not provided or do not comply with the Commission's requests, the Commission may adopt *"common specifications"* for the requirements set out in Article 8-15 and Article 53-55. Where a HRAI System is in conformity with a common specification, it shall be presumed to be in conformity with the requirements in Article 8 -15 and Article 53-55, to the extent that such common specifications cover those requirements.

Strangely Article 41(5) provides that where Providers of a HRAI System or a GPAI Model do not comply with common specifications, they must duly justify that they have adopted technical solutions that meet the requirements in Article 8-15 or, as applicable, Article 55-53 to at least an equivalent level. There is no equivalent obligation in respect of Providers who have failed to comply with a harmonised standard provided by the European standardisation organisations.

C GENERAL PURPOSE AI SYSTEMS and GPAI MODELS

General Purpose AI Systems are defined under the Act as AI systems that are based on a *"general-purpose AI model"* (**GPAI Model**) which have the capability of serving a variety of purposes.

A GPAI Model is defined as *"an AI model … that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications..."*. The definition explicitly excludes AI models that are used before release on the market for the purposes of research, development and prototyping activities.

Recital 97 of the Act notes that the notion of GPAI Models should be clearly defined and set apart from the notion of AI Systems. GPAI Models may be placed on the market in various ways, including through libraries, application programming interfaces (APIs), as direct downloads, or as physical copy. Such models may be further modified or fine-tuned into new models. However, although AI models are essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components, such as for example a user interface, to become "AI systems". AI models are typically integrated into and form part of AI systems.

The Act does not strictly define the criteria for how the generality of a model should be determined, but notes it can be assessed by considering a number of elements, noting for example that models with at least a billion of parameters and trained with a large amount of data using self-supervision at scale should be considered as displaying significant generality and capable of performing a wide range of distinctive tasks. (Recital 98). Large generative AI models are a typical example for a general-purpose AI model (Recital 99).

Interestingly the Act is focused on imposing obligations on GPAI Models rather than on GPAI systems.

Obligations for Providers of GPAI Models

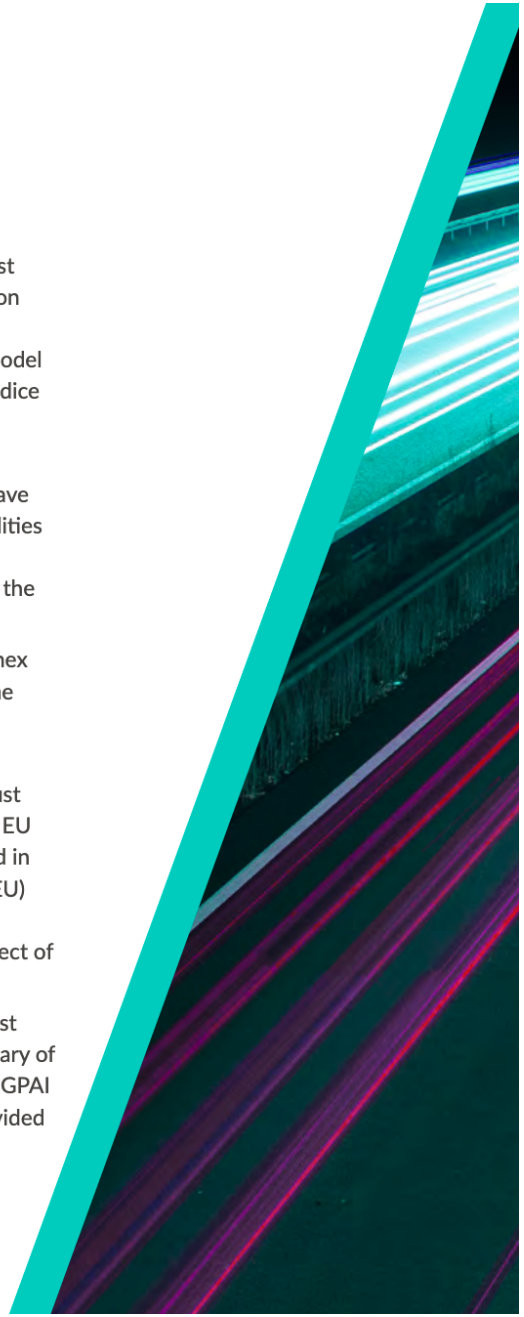
The Act imposes a number of obligations on the Providers of GPAI Models:

a. **Technical Documentation:** Providers must maintain technical documentation on the model, including all of the information required under Annex XI; which includes general descriptions of:
   - » the tasks that the model is intended to perform and the nature of AI systems in which it can be integrated
   - » the acceptable use policies applicable to the model
   - » the date of release and methods of distribution
   - » the architecture and number of parameters
   - » the modality (e.g. text, image) and format of inputs and outputs
   - » the technical means required for the model to be integrated in AI systems
   - » the training and testing process, including training methodologies and data used

b. **Information for Users:** Providers must make information and documentation available to Providers of AI systems who intend to integrate the GPAI model into their AI systems. Without prejudice to intellectual property rights, the information provided must:
   - enable Providers of AI systems to have a good understanding of the capabilities and limitations of the model and to comply with their obligations under the Act
   - provide all of the information in Annex XII, which includes much of the same elements set out in Annex XI (see summary above)

c. **Copyright Compliance:** Providers must put in place a policy to comply with EU copyright law and related rights, and in particular Article 4(3) of Directive (EU) 2019/790 (which relates to express reservation of rights holders in respect of text and data mining).

d. **Training Transparency:** Providers must publish a sufficiently detailed summary of the content used for training of the GPAI model, according to a template provided by the AI Office.



The obligations set out in points (a) and (b) above do not apply to Providers of AI models that are released under a free and open licence, whose parameters are made publicly available. However this exception shall not apply to general-purpose AI models with systemic risks (discussed further below).

Obligations for Providers of GPAI models with systemic risk

The Act classifies certain GPAI Models as having a "systemic risk" and applies greater obligations to the Providers of such models.

A GPAI Model will be classified as having a *"systemic risk"* in two situations:

a. if it has *"high-impact capabilities"* - unfortunately the term *"high-impact capabilities"* is not defined in the Act. It seems this is intended to allow the term to have a dynamic meaning which is reflective of the developing state of the art and which can encompass any GPAI model that could have a significant impact on the internal market due to its possible uses or potential reach. The Recitals state that *"high-impact capabilities"* means *"capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models"* and notes that the full range of capabilities of a model may only become clear after it is placed on the market. The Recitals also note that one of the benchmarks that will be considered to determine if a model has "high impact capabilities" is the cumulative amount of compute used for the training of the GPAI model measured in floating point operations ('FLOPs'). A GPAI model shall be presumed to have *"high impact capabilities"* when the cumulative amount of computation used for its training measured in FLOPs is greater than 10^25, but this threshold may also be amended by the Commission in light of evolving technologies; or

b. the Commission may also issue a decision identifying an individual GPAI Model as carrying a systemic risk. This can be done either ex officio or can be triggered following an alert from the scientific panel established under the Act.

Where a GPAI Model has been determined as having a systemic risk, the Provider of such a model must notify the Commission within 2 weeks after it becomes known that the requirements have been met. A GPAI Model Provider is permitted to demonstrate in its notification that, although it meets the requirements set out in Article 51 in respect of identifying systemic risks, the GPAI Model in question does not present a systematic risk due to its specific characteristics.

The Commission shall maintain a list of GPAI Models with systemic risk and make it publicly available.

The Providers of GPAI Models which are established as having a systemic risk are required, in addition to the obligations for GPAI Models already mentioned above, to ensure the following:

a. **Testing:** Providers must perform model testing and evaluation in accordance with standardised protocols reflecting the state-of-the-art, with a view to identifying and mitigating systemic risk;

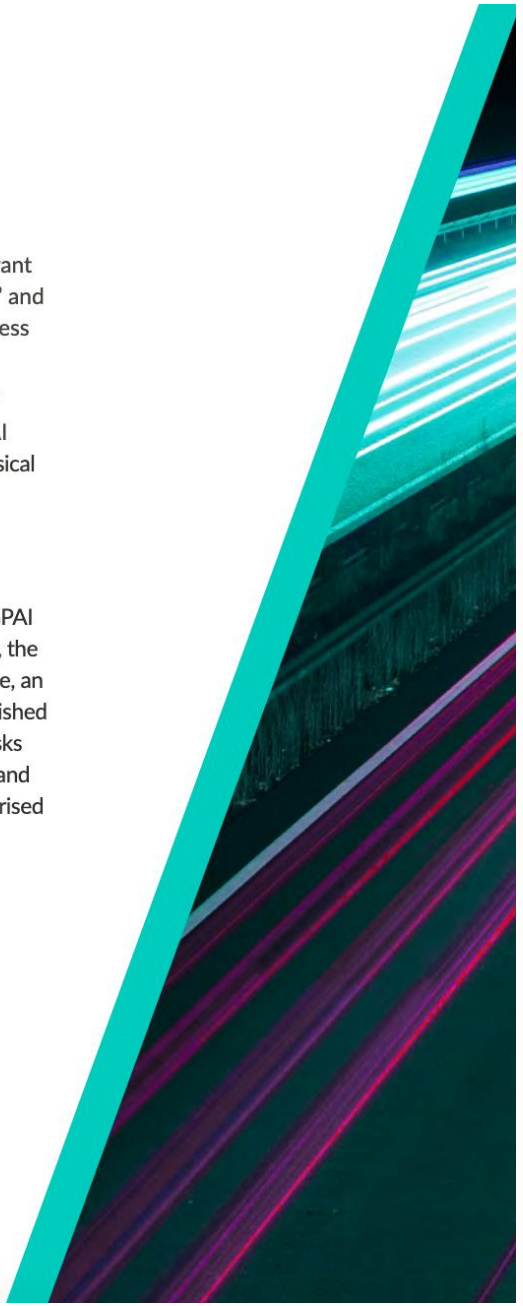
b. **Risk Assessment:** assess and mitigate possible systemic risks at Union level,;

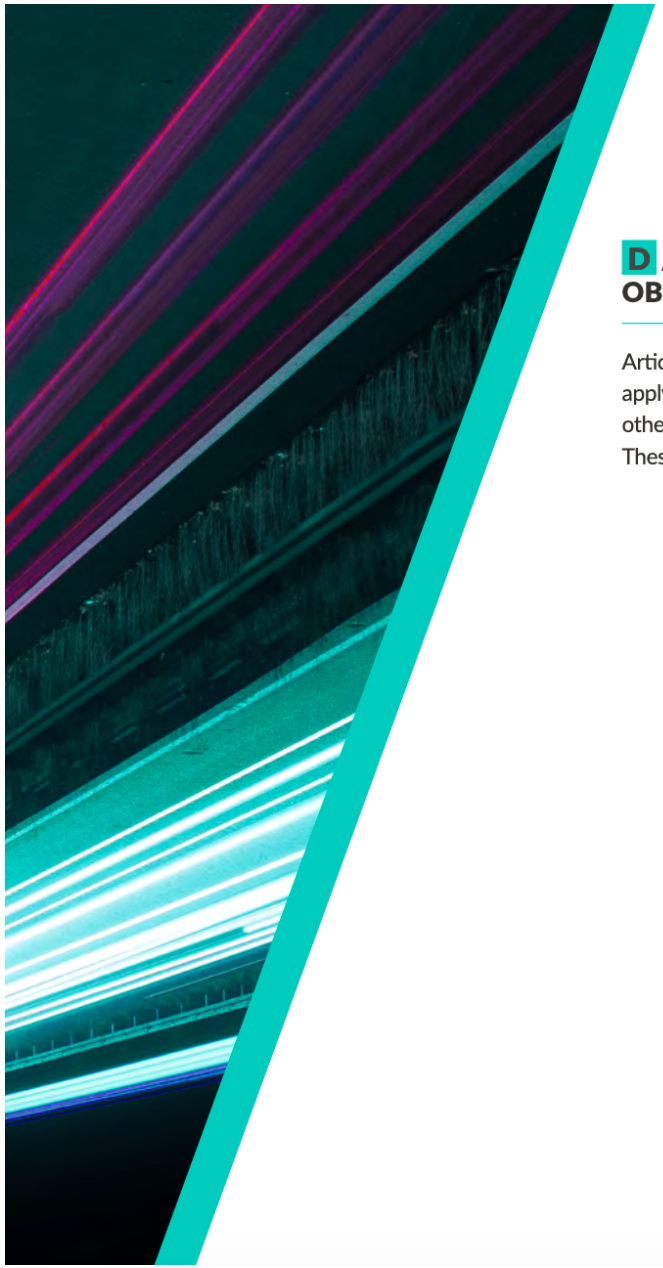
c. **Serious Incident Reporting:** document and report without undue delay to the AI Office and, as appropriate, to national competent authorities, relevant information about "serious incidents" and possible corrective measures to address them;

d. **Security:** ensure an adequate level of cybersecurity protection for the GPAI model with systemic risk and the physical infrastructure of the model.

Authorised Representatives

Under Article 53, where a Provider of a GPAI model is established in a non-EU country, the Provider must appoint by written mandate, an authorised representative which is established in the EU. The Article outlines specific tasks which must be included in that mandate and which the Provider must enable its authorised representative to perform on its behalf.





D ARTICLE 50 TRANSPARENCY OBLIGATIONS

Article 50 sets out a list of obligations which apply to all AI systems, whether high-risk or otherwise, which are used in specific ways. These are as follows:

For Providers

1. **Direct Interaction:** Where an AI system is intended to interact directly with natural persons, Providers must ensure they are designed in such a way that the relevant natural persons should reasonably be made aware that they are interacting with an AI system.
2. **Identifying Content as Created by AI:** Where an AI system can generate synthetic audio, image, video or text content, the Provider of the AI System must ensure that such outputs of the system are marked in a machine-readable format and detectable as artificially generated or manipulated. (This obligation does not apply to the extent the AI systems perform an assistive function for standard editing or does not substantially alter the input data).

For Deployers

1. **Emotion Recognition or Biometric Categorisation:** Where an AI system is used for the purpose for emotion recognition or biometric categorisation, the Deployers of such systems must inform the natural persons exposed to the system of its operation, and must ensure that all personal data processed is done in accordance with the GDPR, EU Regulation 2018/1725 and the Law Enforcement Directive (2016/680), as applicable.
2. **Deep Fakes:** Where AI systems are capable of generating image, audio or video content constituting a "deep fake", the Deployer of such a system must clearly disclose that the content has been artificially generated or manipulated.
3. **Matters of Public Interest:** Where an AI system is used to generate or manipulate text which is published for the purpose of informing the public on matters of public interest, Deployers of such a system must clearly disclose that the text has been artificially generated or manipulated. This obligation shall not apply where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication.

There are limited exceptions to each of the above obligations where the relevant AI system is authorised by law to detect, prevent, investigate or prosecute criminal offences.

SECTION 03
GUIDANCE, SUPERVISION AND ENFORCEMENT FRAMEWORK

The Act introduces quite a complex framework for enforcement. At an EU level, it establishes competencies and roles for two new bodies; the AI Office and the European Artificial Intelligence Board. At a national level, the Act allows a lot of flexibility to Member States in respect of what and how national authorities will be engaged in the supervision and enforcement framework.

New Notified Bodies

i. **AI Office:** The AI Office was established prior to the Act, by way of Commission decision in January 2024. It sits within the Commission and is envisioned as the centre of AI expertise across Europe. Under the Act, the Office will support the uniform implementation and enforcement of the Act among Member States by providing support to and facilitating information exchange between them. It has a range of competencies under the Act including:

- operating as the primary authority responsible for supervision and monitoring of **GPAI model** compliance with the Act
- under Article 56, the AI Office will facilitate the development of, and monitor compliance with, **codes of practice** at EU level in order to contribute to the proper application of the Act, including specifically providing codes for compliance with the obligations of GPAI models under Article 53 and 55, and the obligations regarding the detection and labelling of artificially generated or manipulated content under Article 50(7)
- providing **standardised templates** for areas covered by this Regulation
- maintaining a public record of planned and existing **AI sandboxes**
- together with Member States, encourage and facilitate the creation of **voluntary codes of conduct**, intended to foster the voluntary application of some parts of the Act to all types of AI system, including non-HRAI Systems
- developing template questionnaire to assist Deployers in complying with Article 27 (Fundamental rights impact assessment)

Article 96 Guidelines: As noted above, Article 96 of the Act provides that the Commission must develop guidelines on the practical implementation of the Act, identifying particular areas which should be the focus of such guidance, including:

- the application of the requirements in Article 8-15 and Article 25
- the prohibited practices in Article 5
- the provisions related to substantial modification
- the relationship of the Act with the harmonisation legislation set out in Annex I of the Act and other relevant EU law
- the definition of an "AI system" set out in article 3(1)

Given the AI Office's role within the Commission, one would assume the AI Office would have significant involvement in the development of such guidelines.

ii. **European Artificial Intelligence Board (the "Board"):** Under the Act, the Board shall be composed of one representative per Member State. The European Data Protection Supervisor and the AI Office also attend without taking part in votes. Other national and Union authorities, bodies or experts may be invited to the meetings by the Board on a case by case basis, where the issues discussed are of relevance for them. The Act also provides for the establishment of specific sub-groups within the Board to focus on identified issues.

The Board's primary competence will be advising and assisting the Commission and Member States to facilitate the consistent and effective application of the Act, in a role somewhat similar to the European Data Protection Board. For this purpose, the Board's tasks may include:

- upon the request of the Commission or on its own initiative, issue recommendations and written opinions on any relevant matters related to the implementation of the Act and to its consistent and effective

application, including on the development of any codes of conduct and codes of practice pursuant to the Act.

- contributing to the coordination among national competent authorities responsible for the application of the Act
- sharing technical and regulatory expertise and best practices among Member States
- providing advice on the implementation of the Act, in particular as regards the enforcement of rules on general-purpose AI models
- contributing to the harmonisation of administrative practices in the Member States, including the functioning of regulatory sandboxes, and testing in real world conditions referred to in Articles 57, 59 and 60
- support the Commission in promoting AI literacy

Compliance Systems

The Act also establishes separate but overlapping compliance systems in respect of: (A) AI Systems and (B) GPAI Models.

A AI Systems

The Market Surveillance Regulation

EU Regulation 2019/1020 (the **Market Surveillance Regulation** or **MSR**) is a generic, product-safety regulation which creates harmonised standards and controls across the EU in respect of a defined list of non-food products. It is intended to operate in conjunction with the list of specific product-safety legislation set out in its Annex (the *"Union harmonisation legislation"*). That legislation covers a wide range of products like the Machinery Directive (2006/42/EC), the EMC Directive (2014/30/EU), the Low Voltage Directive (2014/35/EU), the Pressure Equipment Directive (2014/68/EU) etc.

The MSR requires Member States to appoint one or more Market Surveillance Authorities (**MSAs**) to supervise compliance with the Union harmonisation legislation referenced in the MSR, and the additional obligations in the MSR itself, and to take appropriate measures where "economic operators" fail to ensure a product's compliance with those legislative requirements. Ireland has appointed a number of different MSAs focused on different industry sectors, these include the Competition and Consumer Protection Commission, the Road Safety Authority, the Environmental Protection Agency, the Sustainable Energy Authority of Ireland and the Irish Aviation Authority.

Article 74 of the AI Act provides that the MSR shall apply to AI systems covered by the Act. Any reference to *"economic operator"* under the MSR shall be understood as including all "operators" identified under the Article 2 of the Act. Furthermore any reference to a "product" under the MSR shall be understood as including all AI systems falling within the scope of the Act. In this way, the Act seeks to bring AI systems within the MSR framework and make MSAs primarily responsible for monitoring and enforcing compliance with the obligations arising in respect of AI systems under the Act.

Under Article 70 of the Act, each Member State must appoint at least one MSA for the purposes of the Act. Member States must communicate to the Commission the MSAs that have been identified and the tasks assigned to each of those authorities.

In general, Member States will be free to determine which authorities will operate as the MSA in respect of AI systems. Some of the legislation listed in Section A of Annex I (which relate to HRAI systems) designates an authority as responsible for market surveillance but Member States may designate another relevant authority to act as MSA in respect of AI systems, provided the Member States ensure coordination with the relevant sectoral MSA responsible for the enforcement of the legislation in Annex I. For HRAI systems placed on the market or used by financial institutions regulated by EU financial services law, by default, the MSA will be the relevant national authority responsible for the financial supervision of those institutions. However Member States may, where appropriate, also derogate from this position and appoint another authority as MSA for the purposes of the Act.

The Act does prescribe the authority which must serve as MSA in respect of certain types of AI system - for HRAI Systems which are listed in point 1 of Annex III (Biometrics), in so far as the system is used for law enforcement, border management or justice and democracy purposes, and for HRAI Systems listed in

points 6 (Law enforcement), 7 (Migration, asylum and border control management) and 8 (Administration of justice and democratic processes) of Annex III, Member States must designate as MSA either (i) the data protection supervisory authority under the GDPR or (ii) the authority designated pursuant to the Law Enforcement Directive (Directive 2016/680). Where EU institutions and bodies or offices fall within the scope of the AI Act, the European Data Protection Supervisor shall act as MSA, except in relation to the CJEU.

Under the MSR and the AI Act, MSAs have a wide range of investigative and enforcement powers, including requiring operators to take appropriate corrective action in respect of non-compliance and/or requiring the recall or withdrawal of an AI system from the market.

Under Article 85, private individuals who have grounds to believe that an infringement of the Act has occurred may submit a reasoned complaint to the relevant MSA. In accordance with the MSR, such complaints will be taken into account for the purpose of conducting market surveillance activities and shall be handled in line with dedicated procedures.

Notifying authorities and notified bodies

As noted above, Providers of HRAI Systems must complete a conformity assessment of a relevant HRAI System, before it is placed on the market.

The Act provides for two different types of conformity assessment, set out Annexes VI (**Assessment Type 1**) and VII (**Assessment Type 2**) of the Act.

Assessment Type 1 is a purely internal process whereby the Provider must verify the relevant system complies with the general standards in terms of quality management system and the surrounding technical documentation. HRAI Systems referred to points 2-8 of Annex III (see above) must perform this type of conformity assessment and are not required to involve any notified body.

Assessment Type 2 is a more detailed process. As set out in points 4.3 - 4.6 of Annex VII, it involves an assessment by a third party "notified body" of the AI system's technical documentation, as well as any other elements of the system which may be necessary for the notified body to complete its evaluation of conformity with the Act.

Articles 28-38 sets out the rules for the appointment and operation of notified bodies. Essentially notified bodies are independent contractors which have been assessed and approved by Member State authorities (defined a "notifying authorities" under the Act) as appropriate bodies to engage in conformity assessments under the Act. Under Article 70 of the Act, each Member State must appoint at least one notifying authority who will be responsible for approving the authorisation of notified bodies.

Conformity assessments involving a notified body arise in two situations under the Act:

1. Under Article 43(1), where a Provider wishes to complete a conformity assessment in respect of a HRAI System listed in point 1 of Annex III (*Biometrics*), **and** the Provider has been able to apply either harmonised standards or common specifications referred to in Article 40 and 41 respectively, then the Provider may choose whether to opt for Assessment Type 1 or Assessment Type 2. If the harmonised standards or common specifications do not exist or the Provider has not been able to apply them, then the Provider must complete the Assessment Type 2 process.
2. Under Article 43(3), for HRAI Systems covered by the the legislation listed in Section A of Annex I, the Provider must follow the relevant conformity assessment required under those acts, **as well as** points 4.3-4.5 and the fifth paragraph of point 4.6 in Annex VII (i.e. the parts which require involvement of notified bodies).

B GPAI Models

In contrast to AI systems, Article 88 of the Act provides that the Commission shall have exclusive powers to supervise and enforce Article 51-56 - i.e. the provision that impose obligations in respect of GPAI models. The Commission shall entrust the implementation of these tasks to the AI Office.

Under Article 89, the AI Office may take necessary actions to monitor effective implementation and compliance with the Act by Providers of GPAI Models, including their adherence to approved codes of practice.

Under Article 88(2), where appropriate, MSAs may request the Commission to exercise its powers to assist on the fulfilment of their tasks - e.g. where a MSA is unable to conclude an investigation of a HRAI System because of its inability to access information related to the AI model.

Powers of investigation: Under Article 91, the Commission may request the Provider of a GPAI Model to provide any documentation or information necessary to assess compliance with the Act.

Where the information provided under Article 91 is insufficient or where the AI Office deems it necessary to investigate systemic risks at an EU level of GPAI Models with systemic risks, the AI Office may, after consulting with the Board, may conduct an "evaluation" of the relevant GPAI Model, under Article 92. The term "evaluation" as used in Article 92 is not defined, but it seems intended to denote a more in depth investigation than the requests for information made under Article 91. The Commission may decide to appoint independent experts to carry out the evaluation on its behalf. The Commission may also request access to the GPAI Model through its API or further appropriate means including the source code.

Corrective measures: Under Article 93, where necessary and appropriate the Commission may request Providers to:

- take appropriate measures to comply with the obligations set out in Article 53
- require a Provider to implement mitigation measures, where the evaluation carried out in accordance with Article 92 has given rise to serious and substantiated concern of a systemic risk at Union level
- restrict the making available on the market, withdraw or recall the relevant model

Procedural Rights: Article 94 provides that Article 18 of the MSR (which provides a number of procedural rights for economic operators following a regulatory decision) shall apply mutatis mutandis in respect of Providers of GPAI models.

PENALTIES

Article 99 - 101 sets out the rules in respect of the penalties to be imposed following non-compliance with the Act.

A AI Systems

Under Article 99, Member States must lay down the rules on penalties and other enforcement measures applicable to infringements of the Act by Operators and notify the Commission of those rules. Article 99 does outline specific maximum administrative fines which may be applied in respect of different types of violation, as set out in the table below.

Article 99(7) sets out a detailed list of factors which should be considered when determining whether to impose a fine and what the amount should be.

Non-compliance with	Maximum Administrative Fine
Prohibition of AI practices referred to in Article 5	**€35 million** or if the offender is an undertaking, up to **7% of its total worldwide annual turnover** for the preceding financial year, whichever is higher
Obligations of providers pursuant to Article 16	**€15 million** or, if the offender is an undertaking, up to **3% of its total worldwide annual turnover** for the preceding financial year, whichever is higher
Obligations of authorised representatives pursuant to Article 22	
Obligations of importers pursuant to Article 23	
Obligations of distributors pursuant to Article 24	
Obligations of deployers pursuant to Article 26	
Requirements and obligations of notified bodies pursuant to Articles 31, 33(1), 33(3), 33(4) or 34	
Transparency obligations for providers and deployers pursuant to Article 50	
Requirement not to supply incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request	**€7.5 million** or, if the offender is an undertaking, up to **1% of its total worldwide annual turnover** for the preceding financial year, whichever is higher

B GPAI Models

Under Article 101, the Commission may impose an administrative fine on the Providers of GPAI Models of an amount of **€15 million or not exceeding 3% of their annual total worldwide turnover** in the preceding financial year, whichever is higher, where the Commission finds that the Provider intentionally or negligently:

- infringed the relevant provisions of the Act
- failed to comply with a request for a document or for information pursuant to Article 91, or supplied incorrect, incomplete or misleading information
- failed to comply with a measure requested under Article 93
- failed to make available to the Commission access to the general-purpose AI model or general-purpose AI model with systemic risk with a view to conducting an evaluation pursuant to Article 92

SECTION 04
MISCELLANEOUS

A AI Literacy

Article 4 of the Act includes a general requirement for the Providers and Deployers of any type of AI systems to take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

B Measures in support for innovation (Article 57 - 63)

i. **Sandboxes:** Each Member State must establish at least one "AI regulatory sandbox" at a national level, which must be operational within 2 years from the date the Act enters into force.

An 'AI regulatory sandbox' is defined as a controlled framework set up by a competent authority which offers providers or prospective providers of AI systems the possibility to develop, train, validate and test, a new AI system, pursuant to a "sandbox plan" for a limited time under regulatory supervision.

Articles 53-59 sets out rules in respect of the functioning of such sandboxes, including rules around how access will be provided, the length of access, the liability for any damage occurring as a result of experimentation within the sandbox and the management of personal data within such sandboxes.

ii. **Real World Testing:** Article 60 and 61 sets out approved conditions to allow for the testing of HRAI systems within real world conditions. The conditions include specifications in respect of the testing plan which must be created and submitted to the relevant MSA, the transfer of data relating to the test, the length of the testing period, level of oversight required and the type of consent providers are required to obtain from subjects of the testing prior to their participation.

iii. **Smaller enterprises:** Article 62 places a number of obligations on Member States to assist in encouraging SMEs to apply the Act to their operations, including through the provision of training and advice on application. Article 63 allows for microenterprises to comply with certain elements of the quality management system required under Article 17 in a simplified manner, to take account of the relative resources available.

C Scientific panel of independent experts

Article 68 provides that the Commission will establish a scientific panel of independent experts (the "scientific panel") which are intended to support the enforcement activities under the Regulations.

The scientific panel will advise and support the AI Office on a number of tasks including:

- supporting the implementation of the Act as regards to GPAI models
- alerting the AI Office to the possible systemic risks at EU level arising from a GPAI model, in accordance with Article 90
- contributing to the development of tools, methodologies and benchmarks to evaluate the capabilities of GPAI Models and systems
- advising on the classification of GPAI models with systemic risk
- supporting the work of MSAs at their request

The panel members must have a particular scientific or technical expertise in the field of AI, independence from any provider of AI systems of GPAI models and an ability to carry out activities diligently, accurately and objectively.

CONTACT

CONTACT US

Email:
info@assentian.com