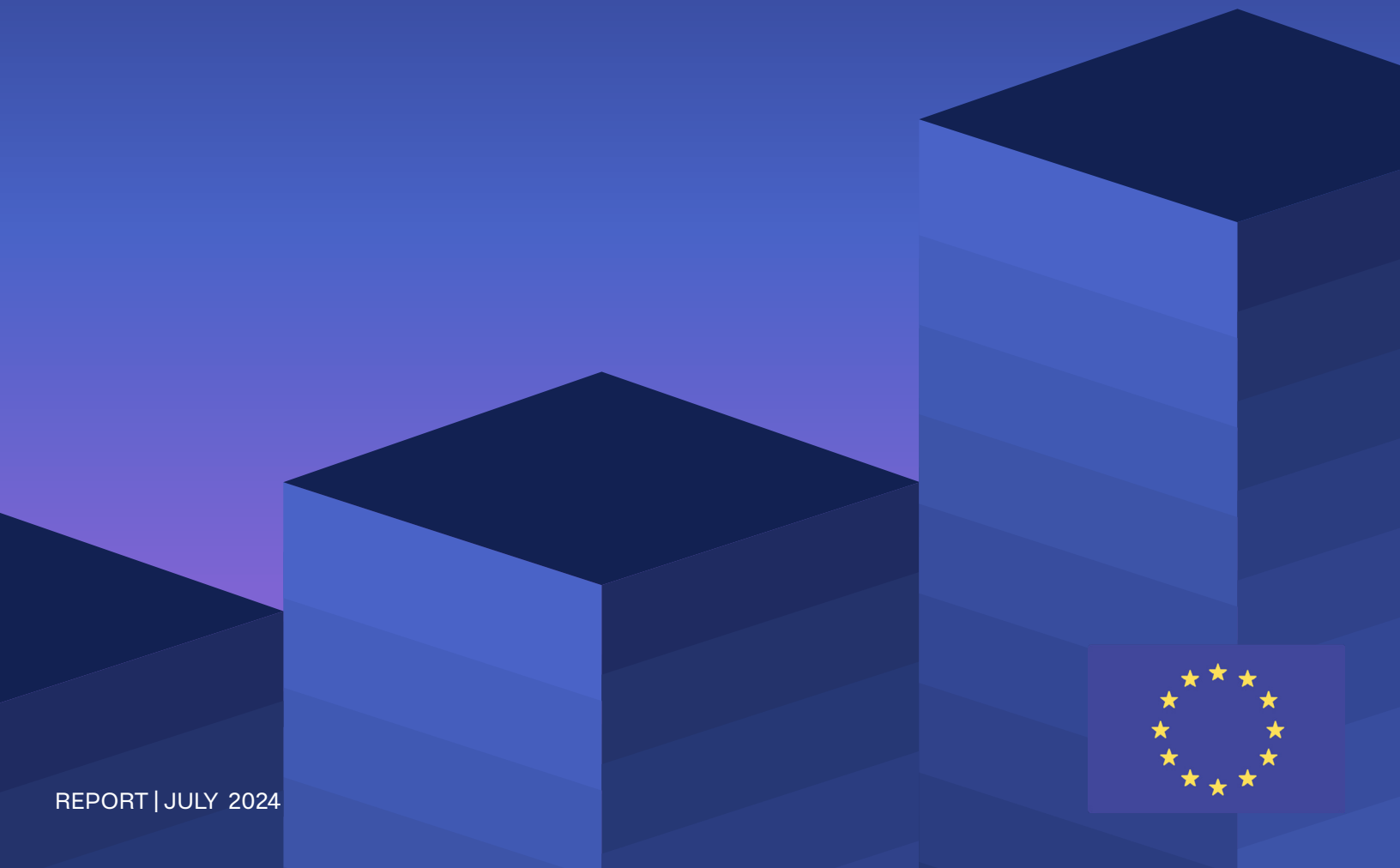
onetrust
DataGuidance

A COMPLETE GUIDE

The EU AI Act



REPORT | JULY 2024

Contributors to this issue

Dominic Wai, Partner at ONC Lawyers

Dominic is a Partner at ONC Lawyers. Before joining the legal profession, Dominic worked in the banking sector, as well as in the Independent Commission Against Corruption (ICAC). Dominic's practice focuses on advising clients on matters relating to anti-corruption, white-collar crime, law enforcement, regulatory and compliance matters in Hong Kong, including advice on anti-money laundering. He also handles cases involving corporate litigation, shareholders' disputes and insolvency matters, defamation cases, domestic and international arbitration cases, cybersecurity, data security and privacy law issues, competition law matters, e-Discovery and forensic investigation issues as well as property litigation.

Melike Hamzaoglu, Partner at Hamzaoglu Hamzaoglu Kinikoglu Attorney Partnership

Melike Hamzaoğlu is a Partner of Hamzaoğlu Hamzaoğlu Kınıkoğlu Attorney Partnership. Her diverse legal practice encompasses areas such as privacy, data protection, cybersecurity, fintech, blockchain, contracts, and various commercial and corporate matters. Melike brings her extensive expertise in privacy and cybersecurity regulations together with a deep understanding of emerging information technologies to provide clients with legal guidance for designing and implementing their products and services. Her knowledge extends to artificial intelligence, robotics, and autonomous driving.

Peter Church, TMT Counsel at Linklaters LLP

Peter is an experienced technology lawyer. He originally studied Computer Science at Cambridge and has nearly 25 years' experience advising clients on the challenges raised by new technology.
He is recognised as an expert in technology regulation in Chambers & Partners and Legal 500, and in the data section of Who's Who Legal. Clients say he "has great experience and insights" and is "excellent on the analysis side of big cases" (Chambers 2024).

Michael Charles Borrelli, COO at AI & Partners

Michael Charles Borrelli is a highly experienced financial services professional with over 10 years of experience. He has held executive positions in compliance, regulation, management consulting and operations for institutional financial services firms, consulted for FCA-regulated firms on strategic planning, regulatory compliance and operational efficiency. In 2020, Michael set-up the operations model and infrastructure for a cryptoasset exchange provider, and has been actively engaged in the Web 3.0 and AI communities over the last 4 years. He currently advises a host of AI, Web3, DLT and FinTech companies.

Table of Content

Table of Content

Introduction

The Artificial Intelligence Act (the AI Act) aims to govern the development, deployment, and use of artificial intelligence (AI) technologies within the EU. The AI Act introduces a risk-based approach, categorizing AI systems based on their potential impact on safety and fundamental rights, with stringent requirements and a conformity assessment process for high-risk AI systems. The AI Act outlines specific prohibitions on certain AI practices deemed unacceptable, such as those posing a clear threat to people's safety, livelihoods, and rights. The AI Act provides for voluntary compliance mechanisms to encourage adherence to ethical guidelines across all AI applications.

A significant aspect of the AI Act is its governance framework, including the establishment of the European Artificial Intelligence Board and national supervisory authorities, to ensure compliance and enforcement. The AI Act emphasizes the importance of post-market monitoring of AI systems and mandates the creation of an EU-wide database for high-risk AI systems.

Application

The AI Act lays down:

- harmonized rules for the placing on the market, the putting into service, and the use of AI systems in the EU;
- prohibitions of certain AI practices;
- specific requirements for high-risk AI systems and obligations for operators of such systems;
- harmonized transparency rules for certain AI systems;
- harmonized rules for the placing on the market of general-purpose AI models;
- rules on market monitoring, market surveillance governance, and enforcement; and
- measures to support innovation, with a particular focus on small and midsize enterprises (SMEs), including start-ups.

SCOPE OF THE AI ACT

The AI Act applies to:

- providers placing on the market or putting into service AI systems or general-purpose AI models in the EU, irrespective of whether those providers are established or located within the EU or in a third country;
- deployers of AI systems that are established or located within the EU;
- providers and deployers of AI systems that are established or located in a third country, where the output produced by the system is used in the EU;
- importers and distributors of AI systems;
- product manufacturers placing on the market or putting into service an AI system together with their product and under their own name or trademark;
- authorized representatives of providers, who are not established in the EU; and
- affected persons that are located in the EU.

Notably for AI systems that are classified as high-risk and related to products covered by EU harmonization legislation, only the following articles of the AI Act apply (Article 2(2)):

- Article 6(1) which identifies which AI systems are considered high-risk;
- Article 57 on the establishment of regulatory sandboxes;
- Articles 102 to 109 which amend various existing regulations to ensure that when rules or standards for different products (like vehicles, security equipment, etc.) are created, they consider the safety and compliance requirements for high-risk AI systems; and
- Article 112 on the review of the list of prohibited AI practices.

Application

Additionally, the AI Act does not change the application of existing EU laws related to:

- personal data processing or the roles and powers of the authorities that oversee data protection compliance (Article 2(7) and Recital 10);
- consumer protection and product safety (Article 2(9)); and
- the liability of providers of intermediary services under the Digital Services Act (DSA) (Recital 11).

Application of the AI Act to existing high-risk AI systems

The AI Act will apply to high-risk AI systems already on the market or in service before its application date only if significant changes in design or intended purpose are made to the system. Public authorities operating AI systems or components of large-scale IT systems must comply by the end of 2030, and by six years after the AI Act's entry into force (Recital 177).

AI SYSTEMS EXCLUDED FROM THE SCOPE OF THE AI ACT

AI systems used for defense (Article 2(3)):

- AI systems exclusively used for military, defense, or national security purposes.
- AI systems not placed on the market or put into service in the EU, where the output is used in the EU exclusively for military, defense, or national security purposes.
- If such systems are used for civilian or other non-excluded purposes, they fall under the scope of the AI Act.

AI systems used in the scope of international agreements (Article 2(4)):

- Public authorities of third countries and international organizations are exempt when acting within the scope of cooperation or international agreements with the EU or its Member States.
- The exclusion applies only if these third countries or international organizations provide adequate protection for fundamental rights and freedoms.

AI systems used for research and development (Article 2(6) and 2(8)):

- AI systems and models developed and used solely for scientific research and development are excluded from the AI Act.
- The AI Act does not apply to any research, testing, or development activities on AI systems or models before they are placed on the market or put into service. Testing in real-world conditions is not covered by this exclusion.

AI systems for personal use

- The AI Act does not apply to deployers who are natural persons using AI systems in the course of a purely personal non-professional activity. (Article 2(10)).

AI systems released under open source licenses

- The AI Act does not apply to AI systems released under free and open source licenses unless they are placed on the market or put into service as high-risk AI systems. (Article 12).

Application

Conditional application (Recital 24)

If an AI system designed for excluded purposes (military, defense, national security) is used, even temporarily, for non-excluded purposes (e.g., civilian, humanitarian, law enforcement), it becomes subject to the AI Act. Further, AI systems designed for both excluded and non-excluded purposes fall under the AI Act.

***Summary note*:**

The AI Act applies to AI system providers and deployers both within and outside the EU. It includes provisions to prevent circumvention of EU laws and ensures that AI systems affecting EU citizens, directly or indirectly, adhere to the AI Act. The AI Act makes exceptions for international cooperation in law enforcement and judicial matters, and specifically excludes AI systems used for research, military, defense, and national security purposes.

Key definitions

The AI Act provides definitions for key terms related to AI systems including:

AI system (Article 3(1)): A 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.

General purpose AI model (Article 3(63)): An AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, 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, except AI models that are used for research, development, or prototyping activities before they are placed on the market.

General purpose AI system (Article 3(66)): Please see section on general purpose system below.

Provider (Article 3(3)): A natural or legal person, public authority, agency, or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places them on the market or puts the system into service under its own name or trademark, whether for payment or free of charge.

A distributor, importer, deployer, or other third party will be considered a provider if they (Article 25(1)):

- put their name or trademark on a high-risk AI system already on the market or in use, unless otherwise stipulated by contract;
- substantially modify a high-risk AI system already on the market or in use, in a way that it remains high-risk; or
- change the intended purpose of an AI system, making it high-risk, if it was not previously classified as such.

For high-risk AI systems that are safety components of products covered by Annex II, Section A of the AI Act, the product manufacturer is considered the provider of the high-risk AI system if (Article 25(2)):

- the AI system is placed on the market with the product under the manufacturer's name or trademark; or
- the AI system is put into service under the manufacturer's name or trademark after the product is placed on the market.

Deployer (Article 3(4): Any natural or legal person, public authority, agency, or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Operator (Article 3(8): Means the provider, the product manufacturer, the deployer, the authorized representative, the importer, or the distributor.

***Summary note*:**

The AI Act provides definitions for key terms, including 'AI System,' 'General Purpose AI System,' 'Provider,' 'Deployer,' and 'Operator.' A provider is defined as any entity that develops, markets, or services an AI system under their name, including third parties who modify or brand high-risk AI systems. A deployer is considered any that uses an AI system under its authority, whereas operators include providers, manufacturers, deployers, authorized representatives, importers, or distributors of AI systems.

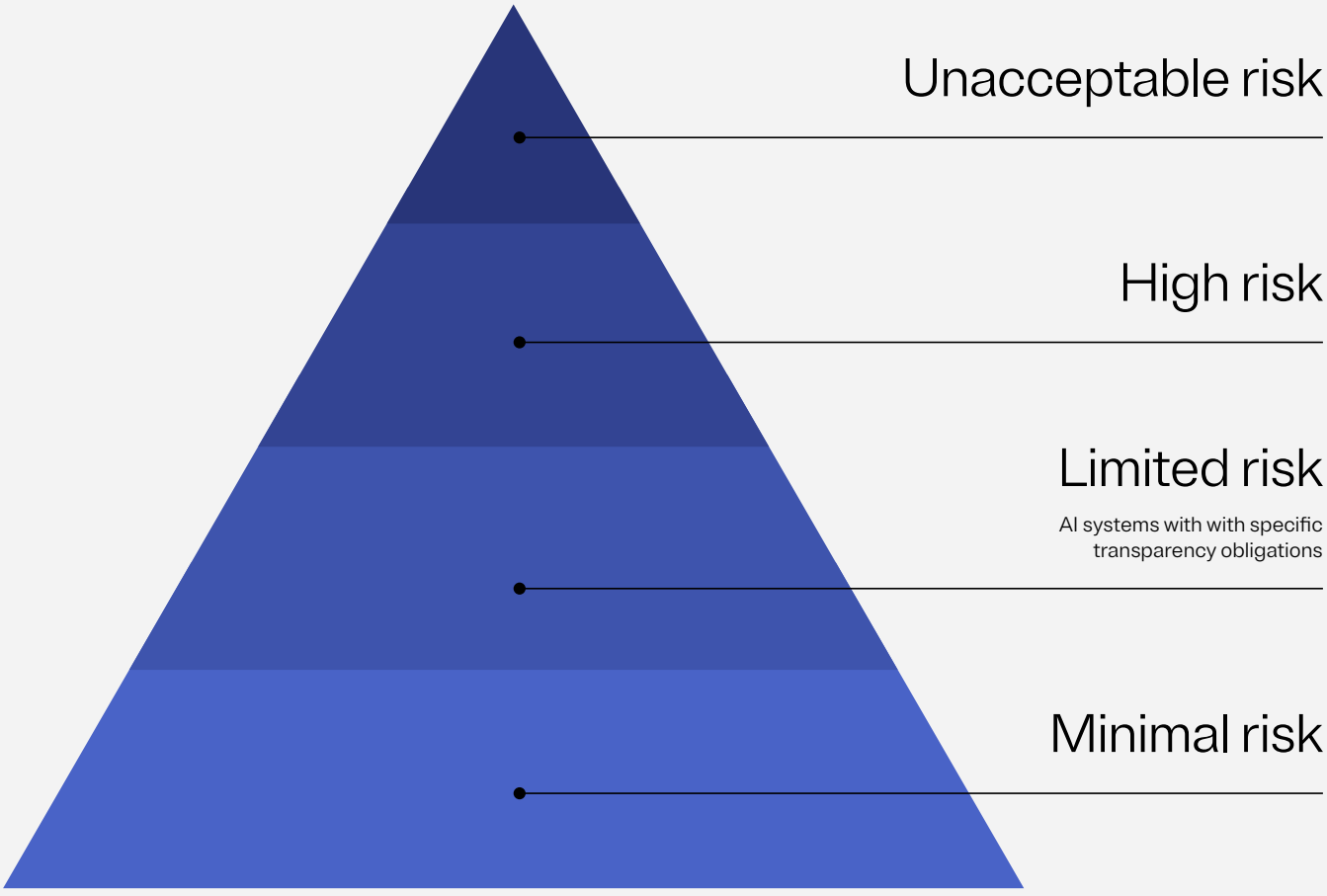
Classification

The AI Act classifies AI systems into four categories based on their levels of risk:

- unacceptable;
- high;
- limited; and
- minimal.

AI systems that pose unacceptable risks to the safety, livelihoods, and rights of individuals are prohibited under the AI Act. High-risk AI systems, which include applications in critical infrastructure, education, employment, essential services, migration, and justice, are subject to stringent requirements under the AI Act, including risk assessments, traceability, documentation, clear information, and human oversight.

Limited-risk AI systems are subject to certain transparency obligations under the AI Act, such as the requirement to inform users when they are interacting with AI and to ensure AI-generated content is identifiable. Minimal-risk AI systems on the other hand can be used freely under the AI Act.



Classification

PROHIBITED AI PRACTICES (UNACCEPTABLE RISK)

The AI Act prohibits the placing on the market, putting into service, or use of AI systems that:

- use subliminal, manipulative, or deceptive techniques that impair a person's ability to make informed decisions and cause, or is reasonably likely to cause, a person to make harmful decisions (Article 5(1)(a));
- exploit vulnerabilities of individuals or groups based on age, disability, or social/economic situations to materially distort behavior, leading to significant harm (Article 5(1)(b));
- provide social scoring of individuals based on social behavior and personal characteristics that lead to detrimental or unfavorable treatment of certain natural persons or groups of persons (Article 5(1)(c));
- predict criminal offenses based solely on profiling or personality traits and characteristics (Article 5(1)(d));
- create facial recognition databases through untargeted scraping of facial images from the internet or CCTV footage (Article 5(1)(e));
- infer emotions of a natural person in the areas of workplace and education institutions except for medical or safety reasons (Article 5(1)(f));
- use biometric categorization systems to profile individuals based on biometric data to infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation (Article 5(1)(g)); or
- are used for real-time remote biometric identification in public spaces for law enforcement purposes except where exceptions apply (Article 5(1)(h)).

Use of biometric identification

The use of 'real-time' remote biometric identification systems in public spaces for law enforcement is generally prohibited unless strictly necessary for specific objectives (Article 5(1)(h)). Before use, authorities must also conduct a fundamental rights impact assessment and comply with national laws, with strict safeguards and limitations on time, location, and individuals involved (Article 5(2)). Further, market surveillance and national data protection authorities must also be notified each time real-time biometric identification systems are used (Article 5(4)).

HIGH-RISK AI SYSTEMS

AI systems are considered high-risk where both of the following conditions are fulfilled (Article 6(1)):

- 'the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the EU harmonization legislation listed in Annex I; and
- the product whose safety component pursuant to point one is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or putting into service of that product pursuant to the EU harmonization legislation listed in Annex I.'

Classification

Annex III of the Act specifies high-risk AI systems mentioned under Article 6(2), including:

- biometrics - emotion recognition, remote biometric identification, or biometric categorization;
- critical infrastructure - safety components in managing and operating critical infrastructure, including digital infrastructure;
- educational and vocational training - decisions like admission, evaluation, or monitoring during tests;
- employment - recruitment, task allocation, monitoring, and evaluation in work-related contexts;
- access to and enjoyment of essential private/public services - credit scoring or creditworthiness evaluation, and risk assessment and pricing in health and life insurance;
- law enforcement - assessing the risk of a person becoming a victim or offender of criminal offenses, evaluating evidence reliability, and profiling in criminal investigations;
- migration – migration, asylum, and border control; and
- administration of justice and democratic process.

AI systems under Annex III are always considered high-risk if the system performs the profiling of natural persons. 'Profiling' means 'any form of automated processing of personal data as defined' under Article 4(4) of the General Data Protection Regulation (GDPR) (Article 3(52)). Notably, the classification of an AI system as high-risk does not automatically classify the product containing it as high-risk (Recital 51).

Notably, AI systems are not considered high-risk if they do not post a significant risk of harm to the health, safety, or fundamental rights of natural persons, including by not materially influencing the outcome of decision-making. One or more of the following criteria must be fulfilled for this (Article 6(3)):

- the AI system is intended to perform a narrow procedural task;
- the AI system is intended to improve the result of a previously completed human activity;
- the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
- the AI system is intended to perform a preparatory task to an assessment relevant for the purpose of the use cases listed in Annex III.

LIMITED-RISK AI SYSTEMS

An AI system that fulfills any of the following conditions may not be considered high-risk as they do not substantially influence decision-making or harm legal interests (Recital 53):

AI systems performing narrow procedural tasks, such as transforming unstructured data into structured data;

AI systems intended to improve the result of a previously completed human activity, providing an additional layer with lowered risk;

AI systems intended to detect decision-making patterns or deviations from prior patterns, following a previously completed human assessment without replacing or influencing it; and

AI systems performing tasks preparatory to an assessment, thus having a very low impact on the assessment to follow.

Classification

The European Commission further clarifies that the AI Act introduces specific transparency obligations for limited-risk AI systems to ensure that humans are informed when necessary. Specifically, providers will have to ensure that AI-generated content is identifiable and AI-generated text published with the purpose of informing the public on matters of public interest must be labeled as artificially generated.

Expert insight

What are the key considerations for evaluating and lowering the risks of AI systems?

Melike outlines that, "the EU AI Act adopts a risk-based approach, imposing varying obligations based on the classification of risk. Therefore, identifying the risk level of an AI system under this Act is crucial. The classification of risk is primarily determined by the system's intended purpose, encompassing its function and specific methods of use. Consequently, the Act prohibits certain AI practices that threaten fundamental rights, such as social scoring, exploitation of vulnerabilities, and the use of subliminal techniques. When an AI system poses potential risks to people's safety or fundamental rights, it is classified as a high-risk AI system and must adhere to a comprehensive set of regulations before it can be introduced to the market. Other AI systems are viewed as minimal risk and can be developed and deployed in compliance with current laws without additional requirements. It is also important to note here that certain AI systems must meet specific transparency requirements, particularly in cases involving a clear risk of manipulation, such as using chatbots."

Additionally, Dominic notes that "for evaluating the risks of AI systems, a thorough risk assessment should be conducted considering:

Purpose and context - understand the intended use and the context in which the AI system will operate;
Potential Impact - assess the potential harm or adverse effects on individuals, society and fundamental rights to humans; and
Technical robustness - evaluate the AI system's reliability, security and accuracy.

For lowering the risks of AI systems, consider the following measures:

Bias mitigation - use diverse and representative datasets to reduce bias in AI systems.
Regular audits and testing - conduct ongoing audits and testing to ensure the AI system operates as intended and complies with legal requirements.
User training - train users on the proper use and limitations of the AI system.
Security measures - implement strong cybersecurity protocols to protect against data breaches and other security threats."

In terms of important steps, under the EU AI Act, Peter explains that "there are two important first steps.

Classification

First, identify the software and hardware products used or provided by your organization and determine if any qualify as an 'AI system'. This may not be straightforward. Some organizations may have hundreds (if not thousands) of affected systems and the definition of 'AI system' is not terribly clear. However, there is likely to be a presumption that some types of technology are AI (such as machine learning) and the European Commission should provide guidance on this concept next year.

Second, determine what 'tier' of regulation applies to that system. Despite the hype, the EU AI Act is arguably 'inch wide; mile deep'. While it imposes very burdensome obligations, they only apply to a relatively narrow class of systems (prohibited, high-risk or GPAI). In practice, many organizations may only have a handful of systems subject to the most burdensome obligations.

For completeness, the EU AI Act does not apply in the UK but has a broad territorial reach, for example it applies if the output of the system is used in the EU. This means it is still likely relevant to UK organizations."

***Summary note*:**

The AI Act classifies AI systems into four risk categories: unacceptable, high, limited, and minimal. Systems with unacceptable-risk, such as those distorting human behavior, using manipulative techniques, or exploiting vulnerabilities, are prohibited. High-risk AI systems, which include applications in critical infrastructure, employment, essential services, and justice, must meet stringent requirements like risk assessments, traceability, and documentation. Limited-risk AI systems are subject to transparency obligations, such as informing users when they interact with AI whereas minimal-risk AI systems can be used freely.

Michael highlights that in terms of evaluating and lowering risks, it's important to "establish a continuous risk management system, identify and analyze foreseeable risks, implement mitigation measures, and ensure compliance through regular testing and updates."

High-risk AI systems

GENERAL REQUIREMENTS

Risk management (Article 9)

High-risk AI systems must establish, implement, document, and maintain a risk management system, understood as an iterative process throughout the AI system lifecycle. The risk management system must involve:

- identification and analysis of known and reasonably foreseeable risks to health, safety, or fundamental rights when used for the intended purpose;
- estimation and evaluation of risks when used as intended and under conditions of reasonably foreseeable misuse;
- evaluation of other possible risks based on the analysis of data gathered from the post-market monitoring system; and
- adoption of appropriate and targeted risk management measures designed to address risks identified.

The risk management measures for high-risk AI systems must ensure that any remaining risks (residual risks) are judged to be acceptable. In this regard, appropriate risk management measures must:

- eliminate or reduce identified risks as technically feasible through adequate design and development of the AI system;
- implement adequate mitigation and control measures to address risks that cannot be eliminated; and
- provide necessary information as required under Article 13 and, if needed, training to deployers.

In managing the risks of high-risk AI systems, the technical knowledge, experience, education, and training of the deployer, as well as the context in which the AI system will be used, should be taken into consideration. High-risk AI systems must be tested to identify the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they comply with the AI Act.

Throughout the AI system lifecycle, privacy and data protection must be guaranteed. This includes applying principles like data minimization and data protection by design and default (Recital 69).

Training, validation, and testing data (Article 10)

For high-risk AI systems involving the training of models with data, the AI Act mandates the use of high-quality datasets for training, validation, and testing. These datasets must undergo appropriate data governance and management practices tailored to the AI system's intended purpose. Key practices include:

- making relevant design choices;
- data collection processes, including the origin and original purpose of data;
- performing data preparation operations such as annotation, labeling, and cleaning;
- updating, enrichment, and aggregation;
- formulating assumptions about what the data should measure and represent;
- assessing the availability, quantity, and suitability of needed datasets; and
- implementing measures to detect, prevent, and mitigate biases.

High-risk AI systems

For the purposes of ensuring bias detection and correction in relation to high-risk AI systems, the providers of such systems may process special categories of personal data, subject to appropriate safeguards, where (Article 10(5)):

- the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymized data;
- the special categories of personal data processed are subject to technical limitations on re-use;
- special categories of personal data are subject to measures to ensure that the personal data processed is secured, protected, and subject to suitable safeguards;
- special category data is not transmitted or transferred to third parties;
- special category data is deleted once the bias has been corrected; and
- the Record of Processing Activities (ROPA) includes a justification on why processing special categories of data was strictly necessary.

Additionally, datasets must be relevant, sufficiently representative, error-free, and complete for the AI system's purpose. They should have appropriate statistical properties as it relates to the persons or groups of persons for which AI system is intended to be used (Article 10(3)). For high-risk AI systems not involving the training of models, the above mentioned requirements only apply to testing datasets.

Expert insight

What data governance best practices can be adopted for training, validation, and testing data?

Peter explains "data quality is key to AI systems given they learn from that data. Organization will need to think carefully about the quality of the data, in particular whether it is accurate, up to date etc. Similarly, for some use cases, it will be really important to ensure that the data does not reflect embedded bias and that it is properly representative. One example is facial recognition systems which have been shown to perform badly on darker-skinned women. This is thought to be because they have been trained on datasets that predominantly contain pictures of white men."

In terms of best practices, Dominic highlighted:

"Data quality and integrity – ensure that the data used is accurate and up to date and verify that the datasets are complete and representative of the real-world scenarios that the AI system will encounter and maintain consistency across all datasets.
Data collection and preparation – ensure that the data gathered is relevant and useful, and properly preprocessed for use.
Data privacy and security – consider data anonymization and encryption to protect the data; implement strict access controls to ensure that only authorized personnel can access the data.
Ensure that the dataset is fair and diverse to avoid bias and discrimination.
Track the data throughout its life cycle to ensure ethical data use, transparency and accountability, and maintain detailed documentation of data sources, preprocessing steps and any modifications made to the datasets.
Data governance policies – establish a data governance framework and clearly define roles and responsibilities for data governance."

Along a similar line, Michael highlights that companies should "ensure data quality, relevance, representativeness, and bias mitigation through proper data collection, processing, and management practices."

High-risk AI systems

Accuracy, robustness, and cybersecurity (Article 15)

High-risk AI systems must be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and perform consistently in those respects throughout their lifecycle. The required accuracy levels and metrics must be included in the AI systems usage instructions. High-risk AI systems should also be resilient to errors, faults, and inconsistencies, especially those arising from interactions with people or other systems, and should include measures like technical redundancy and fail-safe plans. They must also adhere to appropriate standards of cybersecurity to protect against unauthorized access and malicious use.

For systems that continue learning after deployment, measures must be taken to prevent biased outputs from creating feedback loops. High-risk AI systems also need to be protected against unauthorized tampering. This includes cybersecurity measures to prevent, detect, respond to, and resolve attacks like data poisoning, model poisoning, adversarial examples, confidentiality attacks, and other model flaws.

Technical documentation and record-keeping (Articles 11 and 12)

Providers must keep technical documentation for a period of 10 years after the AI system has been placed on the market or put into service and kept up to date. The technical documentation should be drawn up to demonstrate that the high-risk AI system complies with the requirements set in Article 11 and to provide national competent authorities and bodies necessary information to assess the compliance of the AI system applicable requirements.

High-risk AI systems must technically allow for the automatic recording of events (logs) over the duration of the lifetime of the system (Article 12). Providers and deployers of high-risk AI systems must keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable EU or national law, the logs shall be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise (Articles 20 and 29).

Transparency (Article 13)

High-risk AI systems must also be designed and developed in a way to ensure that their operation is sufficiently transparent. Instructions for use of the deployers must be in an appropriate digital format that is concise, complete, and correct, with clear information that is relevant, accessible, and comprehensible to users. Instructions for use must also contain:

- the identity and contact details of the provider;
- characteristics and limitations of the AI system;
- changes to the high-risk AI system and its performance;
- computational and hardware resources needed;
- the expected lifetime of the high-risk AI system and maintenance and care measures;
- a description of the mechanisms included within the high-risk AI system; and
- human oversight measures.

High-risk AI systems

Human oversight (Article 14)

High-risk AI systems should be designed to ensure appropriate human oversight (Article 14(1)). This involves mechanisms that allow human intervention and the ability for humans to understand and control the AI system's functioning.

***Summary note*:**

Generally, high-risk AI systems must incorporate a robust risk management system throughout their lifecycle, focusing on identifying, evaluating, and mitigating risks to health, safety, and fundamental rights. They must use high-quality, representative datasets and maintain high standards of accuracy, robustness, and cybersecurity while ensuring human oversight and control. Providers of such systems must also keep comprehensive documentation and logs to demonstrate compliance and ensure transparency in information provided to deployers.

High-risk AI systems

Providers of high-risk AI systems, or any distributors, importers, deployers, or other third parties considered as providers pursuant to Article 25 of the AI Act, are subject to several obligations, as outlined below.

General obligations (Article 16)

In addition to the general requirements above, providers are required to:

- have a quality management system in place;
- keep the documentation;
- when under their control, keep logs automatically generated by their high-risk AI systems;
- undergo the relevant conformity assessment procedure;
- draw up an EU declaration of conformity;
- comply with the registration obligations;
- take the necessary corrective actions and provide information;
- upon of request, demonstrate the conformity with the high-risk AI system requirements; and
- comply with accessibility requirements.

The measures adopted by the providers to comply with the mandatory requirements should take into account the generally acknowledged state of the art on AI, and be proportionate and effective to meet the objectives of the AI Act (Recital 64).

Provision of contact details (Article 16(b))

The providers must indicate on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation:

- name of the provider;
- registered trade name or registered trademark; and
- the address at which they can be contacted.

Quality management system (Article 17)

Providers must put in place a quality management system and document it in a systematic and orderly manner in the form of written policies, procedures, and instructions. The quality management system must include at least the following:

- strategy for regulatory compliance;
- techniques, procedures, and systematic actions to be used for:
  - the design, design control, and design verification; and
  - the development, quality control, and quality assurance;
- examination, test, and validation procedures to be carried out before, during, and after the development, as well as their frequency;
- technical specifications, including standards, and where relevant, the means to be used to ensure that the high-risk AI system complies with those requirements;

High-risk AI systems

- systems and procedures for data management, including any data operation that is performed before and for the purpose of placing on the market or putting into service high-risk AI systems;
- risk management system under Article 9;
- setting up, implementation, and maintenance of a post-market monitoring system under Article 72;
- procedures related to the reporting of a serious incident under Article 73;
- the handling of communication with national competent authorities and other relevant authorities;
- systems and procedures for record-keeping of all relevant documentation and information;
- resource management; and
- an accountability framework setting out the responsibilities of the management and other staff.

Implementation of the quality management system must be proportionate to the organization's size and respect the degree of rigor and the level of protection required to ensure compliance (Article 17(2)).

Sectoral and financial EU laws

Providers subject to relevant sectoral EU laws can also include the abovementioned aspects as quality management systems pursuant to that law (Article 17(3)).

Financial institutions that have complied with the rules on internal governance arrangements or processes under the applicable EU financial services law are deemed to have fulfilled quality management requirements, except those regarding (Article 17(4)):

- risk management system;
- post-market monitoring system; and
- reporting of a serious incident.

Documentary compliance (Article 18)

Providers must maintain, for 10 years after the high-risk AI system has been placed on the market or put into service, the following:

- technical documentation as described above (Article 11);
- documentation concerning the quality management system (Article 17);
- documentation concerning the changes approved by notified bodies, where applicable;
- decisions and other documents issued by the notified bodies, where applicable; and
- EU declaration of conformity (Article 47).

Member States remain free to determine conditions for the retention of above-mentioned documentation in cases where the provider or its authorized representative goes bankrupt or ceases its activity prior to the end of that period.

High-risk AI systems

Financial EU laws

Financial institutions subject to EU financial services law must maintain technical documents as part of the documentation under the relevant law.

Automatic generation of logs (Article 19)

Providers of high-risk AI systems must keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control. The logs must be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable EU or national law.

Financial EU laws

Financial institutions subject to EU financial services law must maintain the logs automatically generated by their high-risk AI systems as part of the documentation under the relevant law.

Conformity assessment procedure and declaration (Article 43)

Conformity assessment is the process of demonstrating that the requirements set out in Chapter III, Section 2 have been fulfilled. These are requirements include: risk management system, data governance, technical documentation, record keeping, transparency and provision of information, human oversight, and accuracy, robustness, and cybersecurity.

Expert insight

Who should conduct a conformity assessment (e.g., internal or third party)?

The form of conformity assessment required depends on the exact purpose of the high-risk AI system. Some can simply be approved internally based on an internal control review, others will need third party assessment from a notified body.

More specifically, Melike explained "Conformity Assessments can be performed through two methods: internally by the provider or responsible actor, and externally by a notified body. A notified body is an organization designated under the EU AI Act and other relevant EU harmonization legislation to perform third-party conformity assessment activities such as testing, certification, and inspection."

Specifically on third party assessments, Dominic highlights that "third-party assessments are mandatory for AI systems that have a significant impact on fundamental rights, health, safety, or the environment. This includes AI systems used in critical infrastructure, education, employment, law enforcement, migration, and other high-stakes areas."

High-risk AI systems

High-risk AI systems in the area of biometrics in Annex III

A provider of a high-risk AI system in the area of biometrics that has applied harmonized standards under Article 40 of the AI Act or common specifications under Article 41 of the AI Act must base the conformity assessment procedures on one of the following:

- the internal control in Annex VI; or
- the assessment of the quality management system and the technical documentation, with the involvement of a notified body in Annex VII.

Not withstanding, the provider must follow the conformity assessment procedure under Annex VII where:

- harmonized standards do not exist, and common specifications are not available;
- the provider has not applied, or has applied only part of, the harmonized standard;
- the common specifications exist, but the provider has not applied them; or
- one or more of the harmonized standards has been published with a restriction and only on the part of the restricted standards.

The provider may choose any of the notified bodies. However, where the high-risk AI system is intended to be put into service by law enforcement, immigration or asylum authorities, or by EU institutions, bodies, offices, or agencies, the market surveillance authority under Article 74(8) or (9) of the AI Act is the notified body.

Other high-risk AI systems in Annex III

Other high-risk AI in Annex III systems fall into the following areas (point 2- 8 of Annex III):

- critical infrastructure;
- education and vocational training;
- employment, workers management, and access to self-employment;
- access to and enjoyment of essential private and public services and benefits;
- law enforcement;
- migration, asylum, and border control management; and
- administration of justice.

Providers of such high-risk AI systems must follow a conformity assessment procedure based on internal control in Annex VI.

High-risk AI systems covered by the EU harmonization legislation listed in Section A of Annex I

The provider of such high-risk AI systems must follow the conformity assessment procedure required under the applicable legal acts and include the general requirements for high-risk AI systems (Section 2 of the AI Act) in that assessment.

High-risk AI systems

The following provisions of Annex VII also apply to providers of such high-risk AI systems:

- points 4.3 and 4.4 regarding technical documentation;
- point 4.5 regarding granting access to the training and trained models of the AI
- system to the notified body; and
- point 4.6(5) regarding re-training of the AI system prior to the application for a new conformity assessment.

Notified bodies that have been notified under applicable legal acts are entitled to control the conformity of the high-risk AI systems with the general requirements for high-risk AI systems (Section 2 of the AI Act).

Opt-out from a third-party conformity assessment is possible where:

- the legal act in Section A of Annex I provides for such an opt-out; and
- the manufacturer has applied all harmonized standards covering all the relevant requirements; or
- where applicable, the manufacturer has applied common specifications, covering all general requirements for high-risk AI systems (Section 2 of the AI Act).

New conformity assessment

High-risk AI systems must undergo a new conformity assessment procedure in the event of a substantial modification, regardless of whether the modified system is intended to be further distributed or continues to be used by the current deployer.

The following cases are not considered a substantial modification:

- high-risk AI systems that continue to learn after being placed on the market or put into service; and
- changes to the high-risk AI system and its performance that have been pre-determined by the provider at the initial conformity assessment and are part of the information contained in the technical documentation (point 2(f) of Annex IV).

Derogations (Article 46)

Upon a duly justified request, the market surveillance authority within the concerned Member State may issue an authorization for a high-risk AI system to be placed on the market or put into service without carrying out a prior conformity assessment. The authorization would be for a limited period while the conformity assessment is undertaken without undue delay and only if high-risk AI system complies with general requirements for high-risk AI systems (Section 2 of the AI Act).

High-risk AI systems

Expert insight

How do assessments under the AI Act interact with the DPIAs under the GDPR?

Melike highlights that "Assessing the commonalities between GDPR's Data Protection Impact Assessments (DPIAs) and the EU AI Act's two assessments, conformity assessments and Fundamental Rights Impact Assessments (FRIAs), is crucial for organizations to ensure compliance with both regulations when applicable. Before conducting these assessments, it is important to determine an organization's roles under both the GDPR and the EU AI Act, as the same AI system might be subject to varying risk management requirements and classifications under each law. Both the GDPR and the AI Act emphasize risk management. DPIAs focus on the risks to personal data and individuals' privacy, while the AI Act assessments focus on broader risks associated with the use of AI systems, including safety, fairness, and compliance with ethical standards.

Under the GDPR, data controllers are required to conduct DPIAs. In contrast, under the AI Act, it is the providers, not the deployers, who must carry out the conformity assessment before placing a high-risk AI system on the market or putting it into service. Therefore, while a conformity assessment is crucial for organizations developing AI systems, organizations using these AI systems are not required to conduct them under the EU AI Act. However, since providers cannot assess all possible uses of a system, deployers who act as controllers under the GDPR will need to conduct DPIAs for high-risk processing, even if a provider's initial assessment in conformity assessment concludes that the system is not high-risk. On the other hand, DPIAs and FRIAs are much more similar in nature than DPIAs and conformity assessments, as both assess the impact on individuals' fundamental rights and must be conducted by organizations using the system, rather than those developing it."

From a procedural stated point, Peter explains "Detailed risk assessments will be needed for both 'high-risk' or 'systemic risk' GPAIs. The extent to which this overlaps with DPIAs depends on what the AI is used for and who is doing what. Some uses will involve little or no processing or personal data, and hence there will be no need to conduct a DPIA. By way of example, one high-risk use case is the use of AI as a safety component in critical gas or electricity infrastructure – which is not likely to involve processing of personal data under the GDPR. In addition, the risk assessment obligations under the AI Act and GDPR may fall on different people. For a 'high-risk' AI system it is the 'provider' who must conduct the risk assessment. However, it will be the 'deployer' who will actually be using it in practice – and so actually processing applicant's personal data – so will have to conduct a DPAI."

With concluding thoughts, Michael notes "FRIAs under the AI Act complement DPIAs under GDPR, ensuring comprehensive evaluation of data protection and fundamental rights impacts."

High-risk AI systems

***Summary note*:**

The conformity assessment procedures allow the providers to demonstrate compliance with general requirements for high-risk AI systems, namely:

- risk management system;
- data governance;
- technical documentation;
- record keeping;
- transparency and provision of information;
- human oversight; and
- accuracy, robustness, and cybersecurity

Dominic summarizes that:

- Both the GDPR and the AI Act emphasize risk management.
- DPIAs focus on the risks to personal data and individuals' privacy, while the AI Act assessments focus on broader risks associated with the use of AI systems, including safety, fairness, and compliance with ethical standards.
- The AI Act mandates that high-risk AI systems ensure the quality and integrity of datasets, which aligns with GDPR principles of data accuracy and data minimization.
- Both the GDPR and the AI Act place significant emphasis on data governance and security.
- Transparency and accountability are cornerstones of both the GDPR and the AI Act.
- Both the GDPR and the AI Act emphasize the importance of human oversight and ethical considerations.
- Companies deploying high-risk AI systems that process personal data will need to coordinate DPIAs with AI Act conformity assessments.

EU declaration of conformity (Article 47)

The provider must draw up a written, machine-readable, physical, or electronically signed EU declaration of conformity for each high-risk AI system. It must be kept at the disposal of the national competent authorities for 10 years after the high-risk AI system has been placed on the market or put into service.

The EU declaration of conformity must state that the high-risk AI system concerned meets the general requirements set out in Section 2 and include the following information (Annex V):

- AI system name and type and any additional unambiguous reference allowing the identification and traceability of the AI system;
- the name and address of the provider or, where applicable, of their authorized representative;

High-risk AI systems

- a statement that the EU declaration of conformity is issued under the sole responsibility of the provider;
- a statement that the AI system is in conformity and, if applicable, with any other relevant EU law that provides for the issuing of the EU declaration of conformity;
- where an AI system involves the processing of personal data, a statement that that AI system complies with the GDPR and the Directive on Privacy and Electronic Communications (as amended) (the ePrivacy Directive);
- references to any relevant harmonized standards used or any other common specification in relation to which conformity is declared;
- where applicable, the name and identification number of the notified body, a description of the conformity assessment procedure performed, and identification of the certificate issued; and
- the place and date of issue of the declaration, the name and function of the person who signed it, as well as an indication for, or on behalf of whom, that person signed, and a signature.

Furthermore, the EU declaration of conformity must:

- have its copy submitted to the relevant national competent authorities upon request;
- be translated into a language that can be easily understood by the national competent authorities of the Member States in which the high-risk AI system is placed on the market or made available; and
- be kept up to date.

Affix CE marking (Article 16(h))

The provider must affix visibly, legibly, and indelibly the CE marking to the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation.

Furthermore, the CE marking must (Article 48):

- be subject to the general principles under Article 30 of Regulation No. 765/2008;
- in the case of AI systems provided digitally, be easily accessed via electronic means;
- where applicable, be followed by the identification number of the notified body responsible for the conformity assessment procedures set out in Article 43; and
- in the case high-risk AI system is subject to other EU law providing for the affixing of the CE marking, the CE marking must indicate that those requirements are also fulfilled.

Registration (Article 49)

High-risk AI systems in the area of critical infrastructure (point 2 of Annex III)

Such high-risk AI systems must be registered at a national level.

High-risk AI systems

Other high-risk AI systems listed in Annex III (points 1 and 3 - 8 of Annex III)

Who must register and when?

- the provider of the AI system (or the authorized representative): before placing the high-risk AI system on the market or putting into service; and
- deployers that are public authorities, EU institutions, bodies, offices or agencies, or persons acting on their behalf: before putting the high-risk AI system into service or using it.

Where must the registration take place?

The provider and/or the deployer must register themselves and the system in the EU database established by the Commission.

It should be noted that for high-risk AI systems in areas of biometrics, law enforcement, migration, asylum, and border control management (points 1, 6, and 7 of Annex III), registration will be in a secure non-public section of the EU database and must include only the following information, as applicable:

- Annex VIII:
  - section A, points 1-5, 7, and 10;
  - section B, points 1-5, 8, and 9; and
  - section C, points 1-3; and
- Annex IX: points 1, 2, 3, and 5.

AI systems that are not high-risk according to Article 6(3)

Who must register and when?

The provider of the AI system (or the authorized representative) must register it before placing it on the market or putting it into service.

Where must the registration take place?

The provider must register themselves and that system in the EU database established by the Commission.

High-risk AI systems

Corrective actions and duty of information (Article 20)

In the case of suspected non-conformity of the AI system with the AI Act

Providers of high-risk AI systems that consider or have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in conformity with the AI 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; and
- inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorized representative, and importers.

In the case of AI systems presenting a risk within the meaning of Article 79(1)

If a provider becomes aware that an AI system presents a risk to the health or safety, or to the fundamental rights, of persons (understood as 'product presenting a risk' under Article 3(19) of Regulation (EU) 2019/1020), they must immediately investigate the causes in collaboration with the reporting deployer. The provider must also, at the same time, inform the following authorities of the nature of the non-compliance and of any relevant corrective action taken:

- the market surveillance authorities for the high-risk AI system concerned; and
- where applicable, the notified body that issued a certificate under Article 44.

Demonstration of conformity (Article 16(k) and 21) and accessibility requirements (Article 16(l))

Upon a reasoned request of a national competent authority, the providers must demonstrate the conformity of the high-risk AI system with the general requirements for high-risk AI systems under Section 2 by providing all the necessary information and documentation and, if requested, access to the automatically generated logs.

The providers must ensure that the high-risk AI system complies with accessibility requirements in accordance with Directives (EU) 2016/2102 and (EU) 2019/882.

Appointment of an authorized representative in the EU (Article 22)

Third-country providers must appoint an authorized representative established in the EU by written mandate before making their high-risk AI systems available in the EU.

Tasks

The authorized representative can be addressed, in addition to or instead of the provider, on all issues regarding compliance with the AI Act and must be able to, among other things in their mandate:

- verify EU declaration of conformity, technical documentation, and the appropriate conformity assessment procedure;

High-risk AI systems

- ensure documentary compliance including the providers contact details, a copy of the EU declaration of conformity, the technical documentation, and certificate issued by the notified body (if applicable);
- demonstrate the conformity of a high-risk AI system with the general requirements under Section 2;
- cooperate with competent authorities in case of non-compliance or identified risks; and
- comply with registration obligations.

Termination

Where the authorized representative considers or has reason to consider the provider to be acting contrary to its obligations, it shall terminate the mandate and immediately inform the relevant market surveillance authority, as well as, where applicable, the relevant notified body, about the termination of the mandate and the reasons therefor.

Post-marketing monitoring (Article 72)

Providers must establish and document a post-market monitoring system proportionate to the nature and risks of the high-risk AI system to evaluate the continuous compliance of AI systems. Sensitive operational data of deployers that are law-enforcement authorities is out of scope.

The monitoring system must actively and systematically collect, document, and analyze relevant data, including:

- data provided by deployers;
- data collected through other sources on the performance of high-risk AI systems throughout their lifetime; and
- where relevant, analysis of the interaction with other AI systems.

The post-market monitoring system must be based on a post-market monitoring plan, which is part of the technical documentation under Annex IV.

High-risk AI systems under EU harmonization laws (Section A of Annex I)

Where a post-market monitoring system and plan are already established under applicable laws, providers have a choice of integrating abovementioned necessary elements into systems and plans already existing under that legislation.

Financial institutions

The post-marketing monitoring shall also apply to high-risk AI systems for access to and enjoyment of essential private services and essential public services and benefits placed on the market or put into service by financial institutions that are subject to requirements under EU financial services law regarding their internal governance, arrangements or processes.

Reporting of serious incidents (Article 73)

Providers of high-risk AI systems must report any serious incident to the market surveillance authorities of the Member States where that incident occurred.

High-risk AI systems

Timeframe

The report must be made immediately after the provider has established a causal link, or its reasonable likelihood, between the AI system and the serious incident, taking into account the severity of the incident, and a maximum of 15 days after the provider or the deployer becomes aware of the serious incident. However, the period for the reporting must take account of the severity of the serious incident.

In case of a widespread infringement or a serious incident leading to a serious and irreversible disruption of the management or operation of critical infrastructure: the report must be provided immediately, and not later than two days after the provider or the deployer becomes aware of it.

In the event of the death of a person: the report must be provided immediately after the provider or the deployer has established, or as soon as it suspects, a causal relationship between the high-risk AI system and the serious incident and a maximum of 10 days after the date on which the provider or the deployer becomes aware of it.

Where necessary, to ensure timely reporting, the provider or the deployer may submit an initial report that is incomplete, followed by a complete report.

Investigation and cooperation

Following the reporting, the provider must, without delay, perform the necessary investigations regarding the incident, including a risk assessment and corrective action. The provider must not alter the AI system in a way that affects any subsequent evaluation of the causes of the incident prior to informing the competent authorities of such action.

The provider must cooperate with the competent authorities and the notified body concerned during the investigations.

In case of high-risk AI systems subject to EU legislative instruments

For high-risk AI systems referred to in Annex III that are placed on the market or put into service by providers that are subject to EU legal instruments laying down reporting obligations equivalent to the AI Act, the notification of serious incidents shall be limited to the infringement of obligations under EU law intended to protect fundamental rights (Article 3(49)(c)).

High-risk AI systems that are devices or safety components of devices

The notification of serious incidents must be limited to those referred to as serious incidents leading to the infringement of obligations under EU law intended to protect fundamental rights (Article 3, point (49)(c)) and be made to the relevant national competent authority.

High-risk AI systems

Expert insight

What are key considerations for providers of high-risk AI systems?

Melike notes that "Understanding providers' obligations under the EU AI Act is essential due to their pivotal role in the AI value chain, as they face a range of obligations under the Act. Primarily as a pre-market requirement, they must conduct a prior conformity assessment before placing high-risk AI systems onto the market. Following this, they must attach a CE mark to conforming systems, which enables distribution throughout the EU. The other requirements for providers pertain to data and data governance, technical documentation and record keeping, transparency, provision of information to deployers, human oversight, robustness, accuracy, and cybersecurity. As post-market requirements, providers must establish and document a post-market monitoring system that is proportionate to the characteristics of the AI technologies and the risks associated with high-risk AI systems. Such a system should be designed to collect and analyze experience gained from the use of AI systems."

Alternatively, Peter explains that "in some cases, organizations will want to consider removing AI from the system entirely and replacing it with a 'dumb' algorithm. For example, one high-risk use case is the use of AI in recruitment – rather than deal with the burdensome new rules in the EU AI Act it might be just as easy to replace it with a simple rule-based system. If the 'high-risk' AI system is retained, the organisation will need to put a compliance plan in place. This work should start now. While the rule on "high-risk" AI will not apply for two years (or three years for safety products) there is a lot to do in the meantime, such as conduct a risk assessment, prepare technical documentation, go through the conformity assessment process etc."

***Summary note*:**

The AI Act establishes a plethora of requirements for providers of high-risk AI systems including conducting conformity assessments, establishment and maintenance of QMS, incident response, and documentation, among others.

Dominic highlights that "Providers of high-risk AI systems need to consider and adopt:

1. Compliance with regulatory requirements in terms of risk management, data governance, technical documentation and record keeping.
2. Provide clear and accessible information to users about the systems' capabilities, limitations and how it should be used.
3. Human oversight – implement measures to ensure human oversight over the AI system's operation.
4. Technical robustness and safety – this includes system reliability, cybersecurity and resilience measures against attacks to the AI system.
5. Accountability and Responsibility – who should be responsible in the organization for the AI system and compliance to laws and regulations; consider engaging 3rd party auditors to assess and certify the AI system.
6. Ethical considerations.
7. User training and awareness."

High-risk AI systems

Obligations of deployers (Articles 26 and 27)

Monitoring based on the instructions for use

The deployers must take appropriate technical and organizational measures to ensure they use AI systems in accordance with the instructions for use (Article 26(1)). This obligation is without prejudice to other deployer obligations under EU or national law.

Furthermore, the deployers must monitor the operation of the high-risk AI system on the basis of the instructions for use and, where relevant, inform providers (Article 26(5)).

If an AI system is presenting a risk: If the deployer considers that the use of the high-risk AI system in accordance with the instructions may result in that AI system presenting a risk, they must, without undue delay (Article 26(5)):

- inform the provider or distributor and the relevant market surveillance authority; and
- suspend the use of that system.

Serious incident: If the deployer identifies a serious incident, they must immediately inform the provider, the importer or distributor, and the relevant market surveillance authorities. If the deployer cannot reach the provider, they must report the incident to the Member States' market surveillance authorities where that incident occurred following the procedure on reporting of serious incidents mutatis mutandis (Article 26(5)).

This obligation shall not cover sensitive operational data of deployers of AI systems, which are law enforcement authorities.

For financial institutions subject to EU financial services law, the monitoring obligation regarding taking appropriate technical and organizational above will be deemed to be fulfilled by complying with the rules on internal governance arrangements, processes, and mechanisms under the relevant financial service law.

Human oversight

The deployers must assign human oversight to natural persons who have the necessary competence, training, authority, and support (Article 26(2)). This obligation is without prejudice to other deployer obligations under EU or national law.

The deployer is free to organize its own resources and activities for the purpose of implementing the human oversight measures indicated by the provider (Article 26(3)).

Automatically generated logs

Deployers must keep the logs automatically generated by their high-risk AI systems, to the extent such logs are under their control. The logs must be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable EU or national law, particularly on the protection of personal data (Article 26(6).

High-risk AI systems

Financial institutions subject to EU financial services law shall maintain the logs as part of the documentation kept pursuant to the relevant laws.

Duty of information

Prior to putting into service or using a high-risk AI system, deployers must inform workers' representatives and affected workers about deploying high-risk AI systems at the workplace (Article 26(7)). This information must be provided in accordance with applicable laws on information of workers and their representatives.

In the same vein, deployers of high-risk AI systems referred to in Annex III that make decisions or assist in making decisions related to natural persons must inform the natural persons that they are subject to such use of the high-risk AI system (Article 26(11)).

For AI systems used for law enforcement purposes, Article 13 of Directive (EU) 2016/680 applies.

Obligation of registration (for public authorities, EU institutions, bodies, offices, or agencies)

Deployers that are public authorities, EU institutions, bodies, offices, or agencies must register the high-risk AI system at a national level, before putting the high-risk AI system into service or using it (Article 26(8)). Where the high-risk AI system has not been registered in the EU database, deployers must not use that system and inform the provider or the distributor.

Carrying out a DPIA

Where applicable, deployers of high-risk AI systems must use the information provided as part of the transparency obligation of high-risk AI systems under Article 13 to comply with their obligation to carry out a DPIA as foreseen under Article 35 of the GDPR or Article 27 of Law Enforcement Directive.

Cooperation obligation

Deployers must cooperate with the relevant competent authorities in any action taken to implement the AI Act.

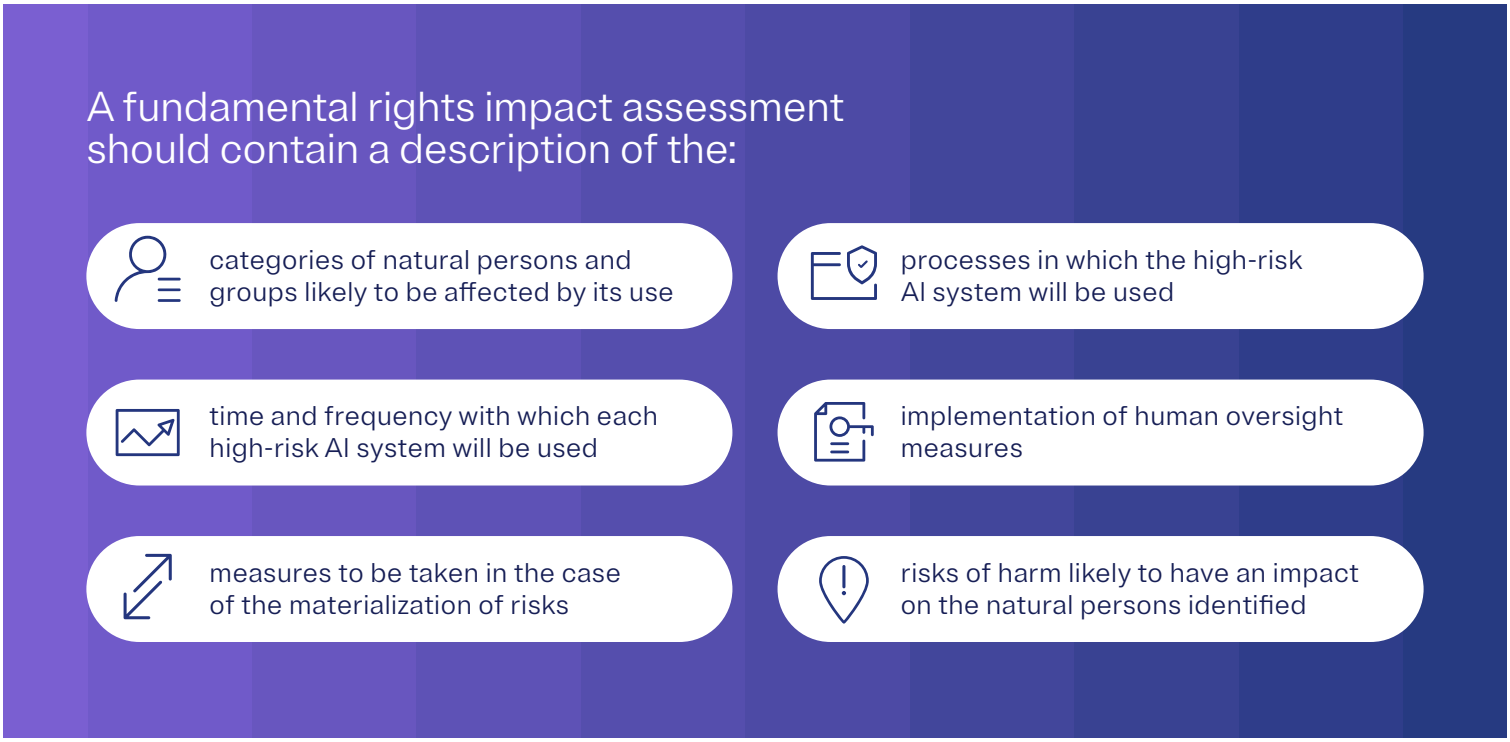
Use of post-remote biometric identification in investigations

With regard to the use of AI systems for investigations of targeted search of persons suspected or convicted of having committed a criminal offense, deployers for post-remote biometric identification must request authorization, ex ante, or no later than 48 hours, by a judicial authority or an administrative authority. Such authorization is not required where the AI system is used for the initial identification of a potential suspect based on objective and verifiable facts directly linked to the offense.

Importantly, the use of such a system is limited to what is strictly necessary for the investigation of a specific criminal offense.

High-risk AI systems

Fundamental rights impact assessment (Article 27)



Timeframe: Prior to deployment.

Concerned high-risk AI systems: High-risk AI systems under Article 6(2). High-risk systems in the area of critical infrastructure are excluded.

Type of deployers:

- Bodies governed by public law.
- Private entities providing public services.
- Deployers of high-risk AI systems in the area of access and enjoyment of essential private and public services intended to be used to evaluate the creditworthiness and credit scores, and for risk assessment and pricing (points 5 (b) and (c) of Annex III).

The fundamental rights impact assessment:

The deployers must perform an assessment of the impact on fundamental rights that the use of such AI systems may produce, and that consists of:

- a description of the processes in which the high-risk AI system will be used in line with its intended purpose;
- a description of the period of time and the frequency with which each high-risk AI system is intended to be used;

High-risk AI systems

- the categories of natural persons and groups likely to be affected by its use in the specific context;
- the specific risks of harm likely to have an impact on the identified natural persons and groups, taking into account the information given by the provider;
- a description of the implementation of human oversight measures; and
- the measures to be taken in the case of the materialization of those risks, including the arrangements for internal governance and complaint mechanisms.

Deployers may, in similar cases, rely on previously conducted fundamental rights impact assessments or assessments carried out by the provider (Article 29a(2)). Assessments must be updated where the deployers believe them not to be up to date.

Deployers must also make the assessment results available to the market surveillance authority unless a derogation from the conformity assessment procedure under Article 46(1) applies.

In cases where the deployer carried out a DPIA under the GDPR or the Law Enforcement Directive, the fundamental rights impact assessment must complement the DPIA in question.

Expert insight

What are key considerations for deployers of high-risk AI systems?

Melike highlights that "One of the key considerations for deployers is the obligation to adhere to the high-risk AI system's instructions provided by the provider, as this significantly affects any potential liability discussion with the provider. Apart from that, deployers are also required to implement human oversight through natural persons who have the necessary competence, training, and authority, as well as the necessary support to monitor both the input data and the system's operation. Additionally, they must retain automated logs for a minimum of six months. In cases where a high-risk AI system is put into service or used 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 high-risk AI system."

Equally, Peter explains "the most important consideration is to remain a 'deployer' and not become a 'provider' (who are subject to much more onerous obligations). For example, if a deployer puts their trademark on the system, substantially modifies it or use it for unexpected persons they will find they are a provider and thus open themselves up too much broader regulation."

High-risk AI systems

***Summary note*:**

Michael highlights that deployers must "perform fundamental rights impact assessments, ensure transparency and human oversight, and maintain compliance with regulatory requirements throughout the AI system's lifecycle."

Along similar lines Dominic notes that "deployers need to:

- understand the AI systems and its risks by conducting risk assessments to identify potential risks associated with deploying the AI system.
- ensure that the AI systems comply with applicable regulatory requirements.
- human oversight and control.
- ensure that the AI system is reliable, monitor its accuracy and protect the AI system with robust cybersecurity protocols and processes.
- transparency and user training.
- ethical and legal considerations to ensure fair and non-discriminatory outcomes.
- accountability and reporting.
- continuous monitoring and improvement to ensure that the AI system can respond to new situations and risks, and to improve its effectiveness and safety."

Obligations of importers (Article 23)

Verifications and documentary compliance

Before placing a high-risk AI system on the market, importers must verify that:

- the relevant conformity assessment procedure has been carried out by the provider;
- the provider has drawn up the applicable technical documentation;
- the system bears the required CE marking and is accompanied by the EU declaration of conformity and instructions for use; and
- the provider has appointed an authorized representative.

Importers must keep, for a period of 10 years after the high-risk AI system has been placed on the market or put into service, a copy of the certificate issued, the instructions for use, and the EU declaration of conformity.

Non-conform AI systems

Where an importer suspects that a high-risk AI system does not conform, is falsified, or is accompanied by falsified documentation, it must not place the system on the market until it has been brought into conformity.

High-risk AI systems

Expert insight

What steps should an importer take to confirm whether a high-risk AI system is falsified, or accompanied by falsified documentation?

According to Peter, "importers will likely rely on the reputation of the relevant provider. Most well-known providers of 'high-risk' AI systems are unlikely to falsify this information given the catastrophic reputational damage. However, in some cases, importers might want to conduct their own due diligence and seek indemnity protection."

Regarding the means of checking for falsification, Michael advises to "verify conformity assessment, technical documentation, CE marking, and EU declaration of conformity."

In the same vein, Dominic outlines that an "importer can consider taking the following measures:

verify the supplier's credentials – reputation check and also check if the supplier is certified or accredited by relevant authorities that ensure adherence to quality and compliance standards;
review the relevant conformity assessment documentation thoroughly;
check with notified bodies – if the AI system requires third-party conformity assessment, contact the notified body to verify the authenticity of the certification and assessment reports;
conduct independent testing – independently test the AI system; and
implement due diligence procedures."

AI systems presenting a risk

Where a high-risk AI system presents a risk, the importer must inform the provider, the authorized representative, and the market surveillance authorities.

On this point, Melike notes that "if the high-risk AI system poses significant risks to health, safety, or fundamental rights as a "product presenting a risk", the importer is obligated to notify the system's provider, authorized representative, and market surveillance authorities. This classification as a "product presenting a risk" denotes a product that could adversely affect health and safety, workplace conditions, consumer protection, environmental integrity, public security, or other public interests beyond acceptable levels under normal use conditions and foreseeable circumstances, including installation, maintenance, and duration of use."

Contact details

Importers must indicate their name, registered trade name or trademark, and their address on the high-risk AI system and on its packaging or accompanying documentation.

High-risk AI systems

Appropriate storage and transport conditions

Importers must ensure that storage or transport conditions do not jeopardize compliance of the AI system under their responsibility.

Cooperation with authorities

Importers must cooperate with the relevant competent authorities and provide, upon a reasoned request, all the necessary information and documentation to demonstrate conformity of the AI system, including technical documentation.

Obligations of distributors (Article 24)

Before making a high-risk AI system available on the market, distributors must verify that:

- it bears the required CE marking;
- it is accompanied by a copy of the EU declaration of conformity and instructions for use;
- the provider and importer have complied with their respective responsibilities;
- the provider included their name, registered trade name or registered trademark, and their address on its packaging or its accompanying documentation, as well as have a quality management system in place (Article 16(b) and (c)); and
- the distributor provided their contact details (Article 23(3)).

Non-conform AI systems

Where a distributor considers or has reason to consider, based on the information in its possession, that a high-risk AI system is not in conformity with the general high-risk requirements, it must not make the high-risk AI system available on the market until it has been brought into conformity.

The distributor must take corrective actions to:

- bring that system into conformity with those requirements;
- withdraw it;
- recall it; or
- ensure that the provider, the importer, or any relevant operator, as appropriate, takes those corrective actions.

High-risk AI system presenting a risk

The distributor must immediately inform the provider or importer of the system and the authorities competent of the high-risk AI system concerned. In particular, the distributor must inform of the non-compliance and of any corrective actions taken.

Storage and cooperation

Distributors have the same obligations regarding contact details, appropriate storage and transportation, and cooperation with authorities as the importers above. In particular, the distributors are expected to provide information and documentation regarding their actions to demonstrate conformity of the AI system.

General Purpose AI Systems

Definition and use of general-purpose AI (GPAI) models (Article 3(66))

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

GPAI models are distinct from AI systems, requiring additional components (like user interfaces) to become AI systems (Recital 97). Large generative AI models, capable of content generation, are typical examples of general-purpose AI models. AI systems integrated with general-purpose models are considered GPAI systems if they serve a variety of purposes (Recital 99).

Systemic risks of GPAI models:

GPAI systems are classified as a GPAI model with systemic risk if it meets any of the following (Article 51(1)):

- it has high impact capabilities on evaluated on the basis of appropriate technical tools and methodologies, including indicators an benchmarks; and/or
- based on the decision of the Commission, ex officio or following a qualified alert by the scientific panel that a GPAI model has capabilities or impact equivalent to the above.

'Systemic risk' is defined as a risk that is specific to the high-impact capabilities of GPAI models, having a significant impact on the internal market due to its reach, and with actual or reasonably foreseeable negative effects on public health, safety, public security, rights, or the society as a whole, that can be propagated at scale across the value chain (Article 3(65)).

These risks increase with the model's capabilities and reach and can arise at any lifecycle stage, with conditions of misuse, model reliability, and model security, among others, influencing the potential risk (Recital 110).

Methodology for classifying systemic risks.

Specifically, 'high-impact capabilities' are defined as GPAI models with capabilities that match or exceed the capabilities recorded in the most advanced general-purpose AI models (Article 3(64)).

The criteria for the designation of a GPAI model with systemic risk is provided under Annex XIII, outlining that the Commission will take into account the number of parameters of the mode, quality, or size of the training data set, the number of business and end users, and if it has a high impact on the internal market, which is presumed to have been reached when it is available to at least 10,000 registered business users in the EU (Annex XIII(f)). A FLOPs threshold is also set to identify high-risk GPAI models, subject to adjustments over time. The Commission can also individually designate a model as having systemic risks based on an overall assessment (Recital 111).

Providers should notify the AI Office, within two weeks, if their model meets the criteria for systemic risks (Recital 112). Further, providers of AI models determined as having systemic risks must identify and mitigate risks, ensure cybersecurity protection, conduct model evaluations, including adversarial testing, and implement risk management policies (Recital 114).

General Purpose AI Systems

Responsibilities of GPAI model providers

Providers of such systems must (Article 53):

- maintain transparency, including up-to-date documentation, and provide information on these models for downstream providers;
- provide technical documentation to the AI Office and national competent authorities;
- make publicly available a detailed summary of the content used for training general-purpose AI models, including copyrighted material (Article 52c(1)(d));
- when placing general-purpose AI models on the EU market, comply with EU law on copyright, regardless of where the copyright-relevant acts occur; and
- appoint an authorized representative prior to placing a GPAI model on the EU market, for providers in third countries.

Providers of GPAI models under open-source licenses with public parameters and model architecture are subject to transparency-related exceptions, unless their models present systemic risks. However, these providers are still required to provide a summary of the content used for model training and comply with EU copyright law (Recital 104).

Cooperation with authorities

Providers of general-purpose AI models must cooperate with the Commission and the national competent authorities.

Expert insight

What are key considerations for providers of general-purpose models?

Peter highlights that "the key first step is to determine if the GPAI has 'high impact capabilities'. If it does it will be subject to significant additional obligations. A GPAI will be presumed to be 'high impact' where its training requires more than 1025 FLOPs but might be deemed high-impact in other cases. The other key concern will be the new obligations to comply with IP laws. Providers will be required to put a global policy in place to comply with EU intellectual property laws, including any expressed reservation of rights (i.e. indication the material should not be used for the training of AIs). Importantly, despite the fact intellectual property rights are granted on a national basis, these rules appear to apply wherever in the world the training takes place."

On the other hand, Melike notes that "providers of general-purpose AI models must prioritize preparing and keeping up-to-date technical documentation for the purpose of making it available, upon request, to the AI Office and the national competent authorities."

General Purpose AI Systems

Obligations of providers of GPAI models with systemic risk

In addition to the aforementioned obligations (and below for authorized representatives), providers of GPAI models with systemic risk must also (Article 55)):

- perform model evaluation in accordance with standardized protocols and tools, including conducting and documenting adversarial testing of the model with a view to identify and mitigate systemic risk;
- assess and mitigate possible systemic risks at the EU level, including their sources, that may stem from the development, placing on the market, or use of GPAI models with systemic risk;
- keep track of, document, and report relevant information about serious incidents and possible corrective measures to address them to the AI Office and, as appropriate, to national competent authorities; and
- ensure an adequate level of cybersecurity protection for the GPAI models with systemic risk and the physical infrastructure of the models.

Providers of GPAI models with systemic risks can use codes of practice to demonstrate compliance with the above obligations until a harmonized standard is published. Providers who do not follow an approved code of practice must demonstrate alternative ways to meet the requirements for the Commission's approval (Article 55 (2)).

Obligations of authorized representatives

An authorized representative must perform tasks as specified in the mandate from the provider and must provide a copy of this mandate to the AI Office upon request. The mandate empowers the representative to (Article 54):

- verify that the technical documentation required of GPAI models has been prepared;
- verify that the provider has fulfilled all their obligations with regard to GPAI models including for models with systemic risks, where applicable;
- keep a copy of the technical documentation available for the AI Office and national competent authorities for 10 years after the model is placed on the market, along with the contact details of the provider;
- provide the AI Office, upon request, with all necessary information and documentation to demonstrate compliance with obligations under the AI Act; and
- cooperate with the AI Office and national competent authorities, upon request, on any action taken regarding the GPAI model with systemic risks, including when the model is integrated into AI systems placed in the market or put into service in the EU.

The mandate will empower the authorized representative to be addressed, in addition to or instead of the provider, by the AI Office or the competent authorities, on issues related to ensuring compliance.

Termination of the mandate

The authorized representative must terminate the mandate if it considers or has reason to consider the provider to be acting contrary to its obligations. In such a case, it must immediately inform the AI Office about the termination of the mandate and the reasons therefor.

General Purpose AI Systems

Exemptions

The obligations above do not apply to providers of general-purpose AI models that are released under a free and open-source license that allows for the access, usage, modification, and distribution of the model, unless the general-purpose AI models present systemic risks.

TRANSPARENCY OBLIGATIONS FOR AI SYSTEMS

Natural persons must be notified that they are interacting with an AI system, unless it is obvious (Article 50(1)). Notification is also required when people are interacting with systems identifying or inferring emotions or categorizing individuals using biometric data (Article 50(3)). The above obligation does not apply to AI systems authorized by law to detect, prevent, investigate, or prosecute criminal offenses, unless those systems are available for the public to report a criminal offense in the latter case.

Providers of AI systems, including general-purpose AI systems generating synthetic audio, image, video, or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated (Article 50(2)). Deployers using AI to generate realistic 'deep fake' content must clearly disclose that the content has been artificially generated or manipulated (Article 50(4)).

The information above must be provided in a clear and distinguishable manner at the latest at the time of the first interaction or exposure and must comply with the applicable accessibility requirements. Of note, the above will not affect the requirements and obligations set out in Chapter III and is without prejudice to other transparency obligations laid down in EU or national law for deployers of AI systems.

Expert insight

What are key considerations for deployers of general-purpose models?

Peter explains, "the deployers of GPAIs will only be subject to very limited obligations under the EU AI Act beyond the 'basic tier' of regulation which is limited to matters such as ensuring AI literacy of their personnel and being transparent where humans can interact with the GPAI or the GPAI creates synthetic content."

Melike further notes that "Deepfakes and Large Language Models (such as ChatGPT) are two examples of general-purpose of AI models. Under the EU AI Act, deployers of AI systems that generate 'deep fakes' must disclose that the content is artificially generated or manipulated. When deep fakes are generated for artistic or creative endeavours, the disclosure obligation still applies. However, such disclosure is required only if it does not hamper the display of the artwork or diminish people's enjoyment of it.

Similarly, those who use AI systems to generate or manipulate text for informing the public on matters of public interest must disclose that the content is artificially generated or manipulated, unless there is sufficient human review or control where a natural or legal person holds editorial responsibility for the publication of the content."

General Purpose AI Systems

***Summary note*:**

Michael states that deployers should "ensure transparency, data quality, and compliance with ethical guidelines; participate in regulatory sandboxes for testing and validation."

Dominic also highlights that: "deployers should consider:

- understanding the AI model and its capabilities.
- risk assessment and management associated with deployment of the AI model.
- ensure compliance with legal and ethical standards.
- transparency and accountability – provide transparent information to users and be accountable to address any issues or complaints related to the AI system's deployment.
- dias detection and mitigation and ensure fairness in deployment.
- human oversight and control
- security of the AI system to protect it from unauthorized access, attacks and data breaches.
- collaborate with AI providers to address any issues, updates or changes related to the AI system.
- continuous improvement."

Training & awareness

Providers and deployers of AI systems must take measures to ensure 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, as well as considering the persons or groups of persons on which the AI systems are to be used (Article 4).

Expert insight

What are key considerations for the development of AI-specific internal risk management frameworks and policies, as well as the establishment of new roles and responsibilities?

Dominic recommends the following:

- "Comprehensive Risk Identification and Assessment – consider a broad spectrum of risks associated with AI systems and relating to the dataset; implement regular risk assessment and involve a diverse group of stakeholders in the risk identification process.
- Establish clear policies and procedures for risk mitigation and governance.
- Create dedicated roles on AI risk management and ethics - form teams that comprise of expertise from different domains to collaboratively manage AI risks and define clear lines of accountability with clear reporting lines and escalation procedures for risk-related issues."

Melike also considers that "to effectively implement the EU AI Act within an organization, an internal risk management framework is essential. Given the potential impacts of AI systems on customers and employees, businesses should establish AI policies to minimize risks and prevent harm. While the creation of new roles like Chief AI Officer and AI Officer is widely discussed, there is no regulated position in the EU Act similar to data protection officers (DPOs) under the GDPR. On the other hand, it is important to recognize that implementing an organization's entire AI strategy and ensuring AI governance is not a task for a single individual. In businesses, management teams are eventually responsible for ensuring AI governance. Legal counsels generally ensure compliance with laws and mitigate legal risks, while audit teams validate data integrity and system functionality to prevent errors and biases. DPOs and privacy teams will be responsible for ensuring compliance with data protection laws when personal data is processed by AI systems."

Finally, Peter adds that "it is important that any policy and governance framework is flexible and able to reflect the four key challenges in this area.

- First, technology is changing fast, and organizations need to react quickly to benefit from it and avoid being left behind in this new technological revolution.
- Second, the regulatory environment is also changing rapidly as more and more jurisdictions adopt specific AI laws.
- The third factor arises from the inherently unpredictable nature of AI. Historically, organizations have had to build their compliance programs around 'people' and 'things.' Most organizations have significant experience trying to regulate the behavior of the former, whilst the latter is normally under the organisation's control. AI is a hybrid between the two and requires new solutions.
- The final factor is the pervasive nature of AI which extends across an organisation's functions and products, making it impossible to confine risk management and compliance to the organization's technology or procurement teams alone."

User Rights

RIGHT TO LODGE A COMPLAINT

Both natural and legal persons have the right to file complaints with the relevant market surveillance authority if they believe that the provisions of the AI Act have been violated (Article 85).

RIGHT TO EXPLANATION OF INDIVIDUAL DECISION MAKING

Persons affected by decisions taken by deployers based on output from high-risk AI systems that have legal or similar adverse effects on their health, safety, and fundamental rights have a right to request the deployer to provide a clear and meaningful explanation of the AI system's role in the decision-making process (Article 86).

The AI Act provides exemption to the above, namely:

- high-risk AI systems used in critical infrastructure; and
- the use of AI systems where exceptions from, or restrictions to, the obligation above follow from EU or national law.

Furthermore, the right to an explanation will apply to the extent that the right is not otherwise provided for under EU law.

AI Regulatory Bodies

The AI Act proposes several AI-related agencies including:

THE AI OFFICE

The AI Office holds the exclusive responsibility for overseeing and enforcing obligations related to GPAI models (Article 88(1)). This includes investigating potential infringements of rules by GPAI model providers (Recital 162).

Specifically, the AI Office has several key tasks which include:

- providing standardized templates for areas covered by the AI Act upon the request of the AI Board;
- developing and maintaining a platform that offers information on the AI Act for all operators across the EU;
- organizing communication campaigns to raise awareness about the obligations under the AI Act; and
- evaluating and promoting best practices in public procurement procedures concerning AI systems.

Furthermore, the AI Office is tasked with:

- Receiving reports of serious incidents involving GPAI models that pose systemic risks (Article 55 (1)(c)).
- Developing codes of practice in collaboration with the scientific community and other experts (Recital 116). Evaluating will evaluate these codes of practice and has the authority to formally approve them or provide common rules for implementation if they are deemed inadequate (Article 52e).
- Developing a template for a questionnaire to facilitate fundamental rights impact assessment (Article 27(5)).
- Evaluating GPAI models to assess their compliance with regulations and investigate the systemic risks of these models, especially after receiving a qualified report from the scientific panel (Article 92 (1)(b)).
- Developing and recommending voluntary model contractual terms between providers of high-risk AI systems and third parties that supply tools, services, components, or processes used or integrated in high-risk AI systems (Article 25(4)).
- Supporting the development of codes of practice to facilitate the effective implementation of the obligations regarding the detection and labeling of artificially generated or manipulated content (Article 50(7)).
- Coordinating joint investigations proposed by market surveillance authorities and the Commission into high-risk AI systems that pose serious risks in multiple Member States (Recital 160).

Additionally, when an AI system utilizes a GPAI model developed by the same provider, the AI Office is charged with monitoring and supervising the system's compliance with regulations. Notably, the AI Office holds powers equivalent to those of a market surveillance authority to carry out these tasks (Recital 161).

AI Regulatory Bodies

EUROPEAN AI BOARD

Composed of Member State representatives, the AI Board will provide advice to the Commission and Member States on the implementation and enforcement of the AI Act. In particular, the AI Board will be responsible for (Article 66):

- contributing to coordination among national competent authorities and supporting joint activities of market surveillance authorities;
- collecting and sharing technical and regulatory expertise and best practices among Member States;
- providing advice on implementing and enforcing the AI Act, particularly for GPAI models;
- contributing to harmonizing administrative practices in Member States, including derogations from conformity assessment, regulatory sandboxes, and real-world testing;
- issuing recommendations and opinions on the development and application of codes of conduct and practices, and evaluating and reviewing the AI Act in certain areas;
- promoting AI literacy, public awareness, and understanding of AI benefits, risks, safeguards, and rights;
- facilitating the development of common criteria and shared understanding among market operators and authorities;
- cooperating with other EU institutions, bodies, agencies, expert groups, and networks in related fields;
- contributing to effective cooperation with third-country authorities and international organizations;
- assisting in developing organizational and technical expertise for implementing the AI Act including assessing training needs;
- supporting national authorities in establishing and developing regulatory sandboxes;
- providing opinions to the Commission on qualified alerts regarding GPAI models; and
- receiving opinions from Member States on qualified alerts and experiences in monitoring and enforcing AI systems.

Additionally, the AI Board is tasked with supporting the Commission in developing practical guidelines for the classification of AI systems (Article 6(5)).

ADVISORY FORUM

The AI Act establishes an advisory forum to provide technical expertise and advise to the Board and the Commission, and to contribute to their tasks. The forum shall be comprised of stakeholders, from industry, start-ups, SMEs, civil society, and academia. At the request of the Board or the Commission, the advisory forum may prepare opinions, recommendations, and written contributions. (Article 67).

NATIONAL COMPETENT AUTHORITIES

Each Member State must designate at least one notifying authority and one market surveillance authority as national competent authorities for overseeing the implementation of the AI Act (Article 70(1)). However, for AI systems used by EU institutions, agencies, offices, and bodies, the national competent authority and market surveillance authority will be the European Data Protection Supervisor (EDPS) (Article 3(48)).

AI Regulatory Bodies

National competent authorities play a role in ensuring the conformity of high-risk AI systems with the requirements under the AI Act. In this regard, they have the power to request all necessary information and documentation from providers of high-risk AI systems and access logs automatically generated by the high-risk AI systems (Article 21(2)).

Additionally, national competent authorities are required to establish at least one AI regulatory sandbox at the national level to facilitate the development and testing of innovative AI systems under regulatory oversight before these systems are placed on the market or otherwise put into service (Articles 57(1) and 57(5)).

National competent authorities may provide guidance, supervision, and support to providers participating in AI regulatory sandboxes on the regulatory expectations and ways providers can fulfill the requirements and obligations under the AI Act (Article 57(7)).

SCIENTIFIC PANEL OF INDEPENDENT EXPERTS

Established by the Commission, the scientific panel is intended to support the enforcement activities under the AI Act. Specifically, the scientific panel shall advise and support the AI Office, in (Article 68(3)):

- the implementation and enforcement of the AI Act with regard to GPAI models and systems, in particular by:
  - alerting the AI Office of possible systemic risks of GPAI models;
  - contributing to the development of tools and methodologies for evaluating capabilities of GPAI models and systems, including through benchmarks;
  - providing advice on the classification of GPAI models with systemic risk;
  - providing advice on the classification of different GPAI models and systems; and
  - contributing to the development of tools and templates;
  - supporting the work of market surveillance authorities, in particular their cross-border activities; and
- carrying out its duties in the context of the safeguard clause.

Enforcement & Remedies

The AI Act grants several powers to national authorities, the AI Office, and the Commission to enforce compliance with its obligations.

ENFORCEMENT OF OBLIGATIONS ON PROVIDERS OF GPAI MODELS

The Commission, through the AI Office, has exclusive powers to supervise and enforce obligations related to GPAI models (Article 88(1)) and monitor the implementation and compliance with the AI Act by providers of GPAI models (Article 89(1)).

POWER OF MARKET SURVEILLANCE AUTHORITIES

Market surveillance authorities are tasked with evaluating high-risk AI systems. If the authority finds that a compliant AI system still presents risks to health, safety, fundamental rights, or other aspects of public interest, it has the power to require the operator to take all appropriate measures to mitigate these risks. The operator must ensure that the AI system no longer presents such risks when placed on the market or put into service, and must do so without undue delay, within a period prescribed by the authority (Article 82(1)).

Furthermore, the market surveillance authority of a Member State has the power to require providers to rectify specific instances of non-compliance, such as improper or missing CE marking, incorrect or absent EU declarations of conformity, failure to register in the EU database, lack of an appointed authorized representative, or unavailable technical documentation. If non-compliance persists, the authority can take measures to restrict, prohibit, recall, or withdraw the high-risk AI system from the market (Article 83).

Market surveillance authorities can request access to the source code of high-risk AI systems, but only if it is necessary to check if the AI system meets certain requirements, and only after all other testing and checking methods using the information provided by the AI system's provider have been tried and found insufficient (Article 74(13)).

POWER TO CONDUCT EVALUATIONS

The AI Office, after consulting the AI Board, has the power to evaluate GPAI models to assess their compliance with regulations and investigate the systemic risks of these models, especially after receiving a qualified report from the scientific panel (Article 92(1)(b)). To conduct the evaluation, the AI Office has the power to request access to the GPAI model concerned (Article 92(3)).

POWER TO REQUEST MEASURES

The Commission, where necessary and appropriate, can request providers to (Article 93(1)):

- comply with obligations for GPAI models;
- implement mitigation measures if an evaluation reveals serious systemic risks at the EU level; or
- restrict, withdraw, or recall the AI model from the market.

Penalties

PROHIBITED AI PRACTICES

Engaging in prohibited AI practices can lead to fines up to €35 million, or for companies, up to 7% of their total global annual revenue from the previous year, whichever amount is greater (Article 99(3)).

NON-COMPLIANCE WITH OBLIGATIONS

If providers, authorized representatives, importers, distributors, deployers, or notified bodies fail to comply with their obligations under the AI Act, they can face fines up to €15 million, or for companies, up to 3% of their total global annual revenue from the previous year, whichever is higher (Article 99(4)).

SUPPLYING INCORRECT INFORMATION

Further, supplying incorrect, incomplete, or misleading information to notified bodies and national competent authorities in reply to a request may lead to fines of up to €7.5 million or, if the offender is a company, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher (Article 99(5)).

Lower fines for SMEs: For SMEs, including start-ups, fines will be the lower of the specified percentages or amounts provided for under the AI Act (Article 99(6)).

CONSIDERATIONS WHEN IMPOSING FINES

When deciding whether to impose an administrative fine and its amount, all relevant circumstances will be considered, including (Article 99(7)):

- the nature, seriousness, and duration of the infringement, its consequences, and the number of affected people and damage suffered;
- whether other market surveillance authorities have already fined the same operator for the same or related infringements;
- the size, annual turnover, and market share of the operator;
- any aggravating or mitigating factors, such as financial benefits gained or losses avoided and the operator's cooperation with authorities;
- the degree of the operator's responsibility and the measures they implemented;
- how the infringement was discovered, especially if the operator reported it;
- whether the infringement was intentional or negligent; and
- actions taken by the operator to mitigate harm to affected individuals.

Penalties

FINES FOR GPAI MODEL PROVIDERS (ARTICLE 101(1))

The Commission may impose on providers of GPAI models fines not exceeding 3% of their annual total worldwide turnover in the preceding financial year or €15 million, whichever is higher, when the Commission finds that the provider intentionally or negligently:

- infringed the relevant provisions of the AI Act;
- failed to comply with a request for a document or for information, or supplied incorrect, incomplete, or misleading information;
- failed to comply with a measure requested under Article 93; and/or
- 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.

The fine amount will depend on the nature, severity, and duration of the violation, adhering to proportionality and appropriateness, and will also consider any commitments made or codes of practice followed.

ENTRANCE INTO EFFECT

The AI Act enters into force on the 20th day following its publication in the Official Journal of the European Union. Although the AI Act applies 24 months following this entrance into force, a series of derogations apply, specifically (Article 113):

- the provisions under Chapter I (general provisions) and Chapter II (prohibited AI practices) apply six months from the AI Act's entrance into force;
- Chapter III Section 4 (notification of authorities), Chapter V (GPAI models), Chapter VIII (EU database for high-risk AI systems), Chapter XII (penalties), and Article 78 (confidentiality) apply 12 months from the entrance into force of the AI Act; and
- the obligations provided for high-risk AI systems will apply 36 months from the entrance into force of the AI Act (Article 113).

onetrust
DataGuidance