ALERT

pillsbury

The EU's AI Act: A Review of the World's First Comprehensive Law on Artificial Intelligence and What This Means for EU and Non-EU Companies

The agreed text of the AI Act was published on July 12, 2024, essentially starting the clock on the legal deadlines contained in it. Its obligations will apply in tiered phases, with the first key obligations being enforced beginning February 2, 2025.

By Steven Farmer, Scott Morton, Mark Booth

TAKEAWAYS

- The EU's AI Act governs AI systems and general-purpose AI models, applying different obligations based on risk.
- Different obligations apply to "providers," "deployers," "importers" and "distributors" of AI systems (all defined).
- The AI Act establishes new EU supervisory bodies to oversee compliance and includes substantial penalties for non-compliance.

07.19.24

Regulation (EU) 2024/1689 (the AI Act) introduces a risk-based framework for regulating AI systems based on how those systems are used, along with a separate framework for regulating general-purpose AI models. Different obligations apply to various actors in the AI supply chain, including providers developing AI systems or GPAI models in the EU, deployers using AI systems in the EU, importers and distributors supplying AI systems into the EU, and product manufacturers incorporating AI systems into

regulated products sold into the EU. The AI Act also applies to providers and deployers whose AI systems or their outputs are made available in the EU, regardless of their location, emphasizing its broad territorial scope and the need for global companies to align with its requirements.

In addition, the AI Act prohibits certain AI use cases which are judged to present unacceptable risk. It also contains specific requirements for "high-risk" AI systems, including risk management, data governance, technical documentation, transparency, human oversight, accuracy, robustness, cybersecurity, and record-keeping. Transparency requirements also apply to certain AI use cases whether or not judged to be "high-risk."

Further detail on the AI Act is set out below.

SCOPE OF APPLICATION

What Does the AI Act Regulate?

The AI Act applies to AI systems and general-purpose AI models (GPAI models).

AI Systems

The AI Act defines an AI system as a machine-based system that is:

i. designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment;

ii. that, for explicit or implicit objectives infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions; and

iii. that can influence physical or virtual environments.

Rather than having a uniform set of requirements for all AI systems, under the AI Act, obligations applicable to AI systems vary based on the risk level of their intended purpose or use (see below).

GPAI models

The AI Act defines a GPAI model as an AI model:

i. trained with a large amount of data using self-supervision at scale;

ii. 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

iii. that can be integrated into a variety of downstream systems or applications.

The GPAI model definition was a late addition to the draft AI Act and was prompted by the relatively recent launch of large language (LLM) model based systems, now widely used in everyday life.

The AI Act identifies a subset of GPAI models as posing a "systemic risk," based on computation power. The obligations applicable to providers of GPAI models (including those that pose a "systemic risk") are set out below.

AI Models Versus AI Systems

The AI Act makes an important distinction between "AI models" and "AI systems":

i. **AI model**. This refers to the algorithm or mathematical model typically trained on large amounts of data through various methods, such as self-supervised, unsupervised or reinforced learning. AI models (including GPAI models) can be provided in various ways including through libraries, through application programming interfaces (APIs) as direct download, or as physical copies. An example of an AI model would be OpenAI's GPT-4o.

ii. **AI system**. Although AI models may be essential components of AI systems, they do not constitute AI systems on their own. AI models require the addition of further components such as, for example, a user interface (used to submit input data and generate output), to become AI systems. AI models are typically integrated into and form part of AI systems. To continue the example, OpenAI's ChatGPT website/app which allows users to submit prompts and receive output is an AI system (GPT-4o is the AI model which powers the AI system).

The AI Act includes obligations applicable to in-scope AI systems. It also includes obligations applicable to AI models, specifically GPAI models and GPAI models that pose systemic risks. These obligations apply when those AI models are made available in the EU on their own or integrated into an AI system.

Exemptions

The AI Act does not apply to the following key activities (amongst other things):

i. AI systems designed or used solely for military, defense or national security purposes, regardless of the entity involved.

ii. AI systems or models, including their output, specifically developed, and used solely for scientific research and development.

iii. Activities related to research, testing or development of AI systems or models before they are made available in the EU. However, this exemption does not apply to testing the AI system or model in real-world conditions (e.g., outside a laboratory or otherwise simulated environment).

iv. AI systems released under free and open-source licenses, unless they are made available in the EU as: (a) high-risk AI systems; (b) prohibited AI systems; or (c) AI systems that are: (1) intended to interact directly with natural persons, (2) that generate synthetic content, or (3) that are emotion recognition systems or biometrics categorization systems).

v. Individuals using AI systems for personal, non-professional activities.

Who Does the AI Act Regulate?

The AI Act applies to several different actors in the AI supply chain and applies obligations depending on the roles each actor plays:

Providers and Deployers

"Providers" and "deployers" of AI systems are the primary actors in the AI supply chain:

i. A **provider** is a party that develops an AI system or a GPAI model or that has an AI system or GPAI model developed and made available in the EU under its own name or trademark, whether for payment or free of charge.

ii. A **deployer** is a party using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.
By way of example, if a company develops an AI screening tool that can assist in the interview and employment process (e.g., by summarizing CV's and scoring applicants), it would generally be a *provider* under the AI Act. Any company that licensed the tool and used it for recruitment would generally be a *deployer*.

Importers and Distributors

"Importers" and "distributors" are entities that make AI systems available in the EU which have been developed by non-EU providers. Importers and distributors are required to ensure that the obligations of the entities higher up the supply chain have been met, and also that they are only reselling compliant AI systems.

i. An **importer** is a party located or established in the EU that supplies an AI system that bears the name or trademark of a party established in a third country.

ii. A **distributor** is a party, other than the provider or the importer, that makes an AI system available in the EU.
Taking the above example, if a provider was based in the United States, selling its AI system via a reseller into the EU, the initial reseller would generally be an importer. Any resellers further down the supply chain would then generally be distributors.

Product Manufacturers

The AI Act also applies to manufacturers that incorporate AI systems as a safety component into products for which current EU regulations already require a third-party conformity assessment. The relevant EU regulations are listed in Annex I to the AI Act.

Where a manufacturer incorporates an AI system in a product which already requires a third-party conformity assessment pursuant to the EU regulations listed in Section A of Annex I to the AI Act, it will be considered a "provider" for the purposes of the AI Act where the product is made available in

the EU under the name or trademark of the manufacturer.

EU regulations listed in Section A of Annex I relate to the following products: cableways, explosives, gas-fueled appliances, lifts, machinery, medical devices, personal protective equipment, pressure equipment, radio equipment, recreational craft personal watercraft and toys.

WHAT IS THE TERRITORIAL SCOPE OF THE AI ACT?

The AI Act includes broad extraterritorial provisions, aiming to regulate AI systems that could directly or indirectly impact individuals in the EU. It applies to:

i. **Providers** that make AI systems or GPAI models available in the EU, regardless of where they are established or located.
ii. **Deployers** of AI systems established or located in the EU.
iii. **Providers** and **deployers** of AI systems where the output produced by the AI System is used in the EU, regardless of where they are established or located.
iv. **Importers** and **distributors** making AI systems available in the EU.
v. **Product manufacturers** that make AI systems available in the EU together with their own products under their name or trademark.
vi. **Authorized representatives** established in the EU of providers that are not established in the EU.

RISK CLASSIFICATION

The AI Act implements a risk-based approach to the regulation of AI systems, categorizing them as follows:

i. unacceptable risk (prohibited AI systems),
ii. high-risk,
iii. limited risk, and
iv. minimal risk.

Compliance obligations correspond to each level of risk.

A separate framework is also introduced in the AI Act for GPAI models and GPAI models posing a systemic risk.

UNACCEPTABLE RISK (PROHIBITED AI SYSTEMS)

The following AI practices are prohibited under the AI Act:

i. **Manipulative AI**. AI systems that use subliminal or deceptive techniques to materially distort a person's decision-making, causing significant harm.

ii. **Exploitative** AI that exploits vulnerabilities of individuals or groups due to age, disability or socio-economic status, with the object of effect of materially distorting behavior leading to significant harm.

iii. **Social scoring**. AI systems that evaluate or classify individuals or groups over time based on social behavior or characteristics, leading to detrimental or unfavorable treatment.

iv. **Risk assessment profiling**. AI systems for making risk assessments of natural persons to predict criminal behavior based on profiling or their personality traits or characteristics (i.e., "predictive policing").

v. **Facial recognition databases**. The creation or expansion of facial recognition databases through untargeted scraping of the internet or CCTV images.

vi. **Emotion inference**. The use of AI to infer emotions of natural persons in workplaces and educational institutions, except for specific medical or safety reasons.

vii. **Biometric categorization**. AI systems categorizing natural persons based on biometric data to deduce or infer sensitive attributes like race, political opinion, or sexual orientation, excluding law enforcement with lawful datasets.

viii. **Real-time biometric identification**. The use of real-time remote biometric identification systems in public spaces for law enforcement, except for in specific circumstances, such as the targeted search for specific victims or missing persons, and provided specific measures are taken.

HIGH-RISK AI SYSTEMS

Classification of High-Risk AI Systems

Two categories of AI systems are considered "high-risk" under the AI Act, namely:

i. All AI systems that are products for which current EU regulations already require a third-party conformity assessment, and all AI systems used as a safety component in such products. The relevant EU regulations are listed in Annex I to the AI Act.

ii. All AI systems intended to be used for purposes listed in Annex III to the AI Act (which will be regularly reviewed and amended as necessary) i.e.:

a. **Biometrics**. AI systems intended to be used: (1) in remote biometric identification systems (i.e., systems used to identify individuals without their active involvement such as based on CCTV footage); (2) for biometric categorization based on sensitive or protective attributes; and (3) for emotion recognition.

b. **Critical infrastructure**. AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity.

c. **Education and vocational training**. AI systems intended to be used to: (1) determine access, admission or assignment of individuals to educational or vocational training institutions at all levels (such as schools or universities); (2) evaluate learning outcomes or education level of individuals; or (3) monitor and detect prohibited behavior of students during tests.

d. **Employment and workers management**. AI systems intended to be used: (1) for recruitment, in particular to place targeted job advertisements, to analyze and filter job applications and to evaluate candidates; (2) to make decisions affecting terms of employment (such as promotion or termination), or to allocate tasks based on individual behavior or personal traits or characteristics; or (3) to monitor and evaluate performance and behavior.

e. **Essential private/public services and benefits**. AI systems intended to be used: (1) to evaluate an individual's eligibility for essential public benefits or services (including health care), as well as to grant, reduce, revoke or reclaim such benefits and services; (2) for risk assessment and pricing in relation to life and health insurance; or (3) to evaluate and classify emergency calls or to dispatch or prioritize emergency first response services, including police, firefighters and medical aid, and used in emergency healthcare triage systems.

f. **Creditworthiness**. AI systems intended to be used to evaluate the creditworthiness of individuals or to establish their credit score, apart from AI systems used for financial fraud detection.

g. **Law enforcement**. AI systems intended to be used by or on behalf of law enforcement: (1) to assess the risk of an individual becoming the victim of crime; (2) as polygraphs or similar tools; (3) to evaluate the reliability of evidence in the course of the investigation or prosecution of crime; (4) for assessing the risk of an individual offending or re-offending not solely on the basis of the automated profiling; (5) to assess personality traits and characteristics or past criminal behavior of individuals or groups; or (6) for profiling persons in the course of detection, investigation or prosecution of crime.

h. **Migration, asylum and border control**. AI systems intended to be used: (1) as polygraphs or similar tools; (2) to assess a risk, including a security risk, a risk of irregular migration, or a health risk, posed by an individual who intends to enter or who has entered the EU; (3) for the examination of applications for asylum, visa or residence permits and for associated eligibility complaints; or (4) in the context of migration, asylum or border control management, for the purpose of detecting, recognizing or identifying individuals, with the exception of the verification of travel documents.

i. **Administration of justice and democratic processes**. AI systems intended to be used: (1) by or on behalf of a judicial authority in researching and interpreting facts and the law and in applying the law to a set of facts, or to be used in a similar way in alternative dispute resolution; or (2) for influencing the outcome of an election or referendum.

An AI system that falls within category (ii) (a) – (i) above may not be considered high-risk if it does not pose a significant risk to natural persons, e.g., if the AI system is intended to perform a narrow procedural task or is intended to improve the result of a previously completed human activity. A provider who considers such an AI system is not high-risk must document the assessment and will still be required to register the AI system. This exemption cannot be applied to an AI system that performs profiling of natural persons, however.

The EU Commission is tasked with publishing a list of example-use cases of AI systems that are high-risk and not high-risk by February 2, 2026.

Obligations Applicable to High-Risk AI Systems

The AI Act sets out the following obligations with respect to high-risk AI systems (as set out in **Section 2, Chapter III of the AI Act**). Providers are primarily responsible for ensuring these particular requirements are met:

i. **Risk management**. A documented risk management system must be created, maintained and regularly updated throughout the lifecycle of a high-risk AI system.

ii. **Data and data governance**. Datasets used to train high-risk AI systems must meet certain quality criteria and be subject to appropriate data governance and management practices.

iii. **Technical documentation**. Technical documentation must be prepared before a high-risk AI system is made available in the EU and must be kept up-to-date. Such documentation must demonstrate that the AI system complies with the requirements of the AI Act and provide authorities with clear and comprehensive information to allow them to assess such compliance.

iv. **Record-keeping (automated logs)**. Such systems must allow for the automated recording of events (logs) throughout the lifecycle of the system.

v. **Transparency and provision of information to deployers**. Providers of high-risk AI systems must provide instructions to enable deployers (i.e., users) to interpret the system's output and use it appropriately.

vi. **Human oversight**. Such systems must be designed and developed in such a way (including with appropriate interface tools) that they can be subject to effective human oversight throughout their use to identify, prevent and minimize risk.

vii. **Accuracy, robustness and cybersecurity**. Such systems must have an appropriate level of accuracy, robustness and cybersecurity to allow them to operate consistently throughout their lifecycle.

Section 3, Chapter III of the AI Act then goes on to set out further obligations applicable to providers, deployers, importers and distributors of high-risk AI systems, as follows.

Providers of high-risk AI systems must comply with the following:

i. **Compliance with Section 2**. Providers must demonstrate such conformity upon a request of a competent authority in an EU Member State, which includes providing: (a) all information and documentation necessary to demonstrate such conformity in an official language used in the Member State concerned; and (b) access to automatically generated logs under the provider's control.

ii. **Information**. Include their name and contact details on the AI system, or when not possible, on packaging or in accompanying documentation.

iii. **Quality management system**. Maintain a proportionate documented quality management system, including policies, procedures and instructions, that ensures compliance with the AI Act.

iv. **Documentation keeping**. Maintain documentation for 10 years after the high-risk AI system is made available in the EU, including (amongst other things) technical documentation (discussed above), documentation concerning the quality management system, and the EU declaration of conformity.

v. **Automatically generated logs**. When the high-risk AI system is under the provider's control, retain automatically generated logs (discussed above) for a period appropriate to the intended purpose of the AI system and for at least six months (unless prohibited under EU law, including the GDPR).

vi. **Conformity assessment**. Ensure the high-risk AI system undergoes the relevant conformity assessment procedure prior to being made available in the EU.

vii. **EU declaration of conformity**. Prepare a signed EU declaration of conformity for each high-risk AI system and retain it for 10 years after the AI system has been made available in the EU.

viii. **CE marking**. Affix the CE marking to the high-risk AI system or where not possible, on its packaging or its accompanying documentation, to indicate conformity with the AI Act.

ix. **Registration**. Before a high-risk AI system is made available in the EU, the provider or, where applicable, the authorized representative, must register themselves and their AI system in the EU database for high-risk AI systems maintained by the European Commission (subject to exceptions).

x. **Corrective actions and duty of information**. Where a provider considers that a high-risk AI system it has made available in the EU does not conform with the requirements of the AI Act, it must immediately take necessary actions to: (a) bring that system into conformity, (b) withdraw it, (c) disable it or (d) recall it, as appropriate.

xi. **Accessibility requirements**. Ensure high-risk AI systems comply with accessibility requirements for people with disabilities under EU law.

xii. **Appoint an authorized representative**. Prior to making their high-risk AI systems available in the EU, providers not established in the EU must appoint an EU-based authorized representative.

Further, **Deployers** of high-risk AI systems must:

i. **Comply with instructions**. Take appropriate technical and organizational measures to ensure they use high-risk AI systems in accordance with instructions for use accompanying the high-risk AI system (made available by the provider).

ii. **Human oversight**. Assign human oversight over the high-risk AI system to persons who have the necessary competence, training, authority and necessary support.

iii. **Input data**. To the extent the deployer exercises control over the input data, it shall ensure that input data is relevant and sufficiently representative given the intended purpose of the high-risk AI system.

iv. **Monitor**. Monitor the operation of the high-risk AI system based on the instructions for use.

v. **Notification**.

a. Where a deployer considers that use of the high-risk AI system as instructed may present a risk to health and safety or the rights of individuals, it must **without undue delay** inform the provider or distributor and the relevant market surveillance authority and must suspend the use of that system.

b. Where a deployer has identified a **serious incident**, it must also immediately inform first the provider, and then the importer or distributor and the relevant market surveillance authorities of that incident.

vi. **Automatically generated logs**. Keep logs automatically generated by the high-risk AI system to the extent such logs are under their control, for a period appropriate to the intended purpose of the AI system and for at least six months (unless prohibited under EU law, including the GDPR).

vii. **Employee notices**. Before using a high-risk AI system in 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.

viii. **Data protection impact assessment (DPIA)**. Where applicable, carry out a data protection impact assessment under Article 35 of the GDPR.

ix. **Transparency**. Where high-risk AI systems are used to make decisions or assist in making decisions related to individuals, inform those individuals that they are subject to the use of the high-risk AI system.

x. **Cooperation**. Cooperate with the competent authorities in any action those authorities take in relation to the high-risk AI system to implement the AI Act.

xi. **Fundamental rights impact assessment**. Where the deployer is: (a) a public body; (b) a private body providing public services; or (c) using a high-risk AI system to assess creditworthiness or for risk assessment and pricing in relation to life and health insurance, perform an assessment of the impact on fundamental rights that the use of the high-risk AI system may produce.

Furthermore:

Importers of high-risk AI systems must ensure that the system conforms with the requirements of the AI Act. Importers must also label the AI system and its packaging or accompanying documentation with their contact information, ensure safe storage and transport, and retain documentation, like the conformity certificate and instructions, for 10 years after the high-risk AI system is made available in the EU. Importers must also provide necessary information to demonstrate compliance upon request from competent authorities and cooperate with them to address any risks associated with the AI systems they import.

Distributors must verify: (i) a high-risk AI system bears the required CE marking and is accompanied by a declaration of conformity and instructions for use; and (ii) that the provider and importer (as applicable) have complied with their respective obligations.

LIMITED RISK AI SYSTEMS (TRANSPARENCY OBLIGATIONS AND "DEEP FAKES")

The AI Act sets out transparency obligations which are applicable to both providers and deployers of AI systems in certain circumstances:

i. **Providers** must ensure that AI systems **intended to interact directly with natural persons** are designed/developed so that users are informed that they are interacting with an AI system. This does not apply to certain AI systems used for law enforcement.

ii. **Providers** of AI systems **generating synthetic audio, image, video or text content** must ensure outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated.

iii. **Deployers** (users) of an **emotion recognition system or a biometric categorization system** must inform the natural persons exposed thereto of the operation of the system and must process personal data in accordance with the GDPR.

iv. **Deployers** (users) of an AI system that **generates or manipulates image, audio or video content constituting a *deep fake***, must disclose that the content has been artificially generated or manipulated.

v. **Deployers** (users) of an AI system that **generates or manipulates text which is published with the purpose of informing the public on matters of public interest** must disclose that the text has been artificially generated or manipulated (subject to exceptions).

MINIMAL-RISK AI SYSTEMS

AI systems that do not fall within the **prohibited**, **high-risk** or **limited-risk** categories are considered **minimal-risk** systems and are not subject to specific obligations under the AI Act (but remain subject to any existing laws that may apply).

For example, commercially available email spam filters may utilize AI to identify and respond to new spam campaigns, but such systems would not generally be regulated under the AI Act.

GPAI MODELS

The requirements applicable to GPAI models are set out in Chapter V of the AI Act. The following obligations are applicable to **providers** of GPAI models:

i. **Technical documentation to authorities**. Maintain technical documentation on the GPAI model and make the same available to the AI Office and national competent authorities.

ii. **Technical documentation to downstream providers**. Make available technical documentation to AI system providers who intend to use the GPAI model, which enables them to understand the capabilities and limitations of the GPAI model and to comply with the AI Act.

iii. **EU copyright law**. Maintain a policy to ensure compliance with EU copyright law.

iv. **Cooperation**. Cooperate with the European Commission and national competent authorities.

v. **Training data**. Publish a summary of the content used for training the GPAI model, using a template provided by the AI Office.

vi. **Appoint an authorized representative**. Prior to making their GPAI model available in the EU, providers not established in the EU must appoint an EU-based authorized representative.

The requirements set out in (i) and (ii) above do not apply to open-source GPAI models in some circumstances, provided they do not present systemic risks.

Additional compliance obligations apply to providers of GPAI models which present systemic risk. These include:

i. **Model evaluation**. Performing model evaluation including adversarial testing of the model to identify and mitigate system risk.

ii. **Systemic risk**. Assessing and mitigating systemic risks at the EU level. Providers must monitor, document and report serious incidents and possible corrective measures to address them.

iii. **Cybersecurity**. Ensuring an adequate level of cybersecurity protection for the model and physical infrastructure.

While the AI Act does not contain specific obligations on deployers of GPAI models, where those models are incorporated into an AI system (e.g., via an API), the entity responsible for that AI system would generally be a provider of the AI system (i.e., a downstream provider) and the obligations applicable to providers would apply in those cases. The provider of the GPAI model would still be subject to the above obligations in this scenario, particularly concerning information which must be provided to AI system providers who intend to use the GPAI model within their AI system to enable compliance with the AI Act.

NEW SUPERVISORY BODIES

The AI Act establishes several new EU bodies responsible for monitoring the EU's approach to AI regulation. The new bodies will work with the European Artificial Intelligence Office (AI Office), established to monitor and investigate AI risks and possible infringements of the AI Act. The new bodies established by the AI Act include:

i. **The European AI Board**. The AI Board shall advise and assist the EU Commission and the Member States to facilitate consistent and effective application of the AI Act. The AI Board is composed of one representative from each EU Member State who has the relevant competences and powers in their Member State to contribute actively to the AI Board's tasks.

ii. **The Advisory Forum**. The AI Act calls for the establishment of an Advisory Forum to provide technical expertise and advice to the Board and the EU Commission. The Advisory Forum shall represent a balanced section of stakeholders including industry, start-ups, small- and medium-sized enterprises, civil society and academia.

iii. **The Scientific Panel**. The AI Act also requires the EU to establish a Scientific Panel, made up of independent experts, intended to support the implementation and enforcement of the act. In particular, the Scientific Panel shall alert the AI Office of possible systemic risks of GPAI model, provide advice on the classification of AI models and systems, and support cross-border market surveillance activities. EU Member States may call upon the experts of the Scientific Panel to support their enforcement activities under the AI Act.

iv. **National Competent Authorities**. Each Member State must also establish or designate at least one notifying authority and at least one market surveillance authority. The notifying authority will be responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies and for their monitoring, while the market surveillance authority shall be responsible for market surveillance, investigation and general enforcement of the AI Act.

PENALTIES

The AI Act includes a raft of potential administrative fines for violations of its requirements, in addition to other enforcement measures such as warnings and non-financial penalties. The penalties levied by Member States must be effective, proportionate and dissuasive. The maximum penalties set out in the AI Act are:

i. **€35m or 7% of worldwide annual turnover** for use of a prohibited AI system;

ii. **€15m or 3% of worldwide annual turnover** for non-compliance with other obligations, including: (a) obligations applicable to high-risk AI systems; (b) obligations applicable to limited risk AI systems, i.e., the transparency obligations; and (c) obligations applicable to providers of GPAI models (which are enforced by the European Commission); and

iii. **€7.5m or 1% of worldwide annual turnover** for the supply of incorrect, incomplete or misleading information to regulators in response to a request.

For large organizations, the maximum fine shall be the greater of the percentage or amount referred to above while for start-ups and SMEs, the fine shall be the lower of the percentage or amount.

The AI Act does not include rights for individuals or organizations to claim damages for harm that they have suffered by virtue of a breach of the AI Act. However, the AI Act is intended to be complemented by the proposed AI Liability Directive and the revised Product Liability Directive. The AI Liability Directive is a proposed piece of EU law that is aimed at reducing legal uncertainty around AI-related damage and ensuring that victims of harm can seek effective redress for such damage. The Product Liability Directive is an existing (but almost 40-year-old) EU law that includes consumer protection rules enabling individuals to seek redress for damages suffered. On March 12, 2024, the EU Parliament adopted a revised version of the Product Liability Directive that reflects the increase in online shopping and the use of emerging technologies such as AI. The updated directive modernizes the EU's approach to consumer redress in

several areas, including to ensure it is appropriate for a society where AI use is more prevalent. While claims may not be brought under the AI Act directly, organizations operating in the AI ecosystem should understand their potential liabilities under these acts.

TIMELINE FOR IMPLEMENTATION

The AI Act will come into force on the twentieth day following its publication, i.e., on August 2, 2024. The operative provisions will then apply as follows:

i. **February 2, 2025**: The ban on prohibited AI systems goes into effect;

ii. **August 2, 2025**: Obligations on providers of GPAI models go into effect;

iii. **August 2, 2026**: Remaining obligations go into effect; and

iv. **August 2, 2027**: Obligations on: (a) AI systems that are products for which current EU regulations already require a third-party conformity assessment; and (b) all AI systems used as a safety component in such products, go into effect.

The AI Act also contains certain "grandfathering" provisions applicable to AI systems and GPAI models already made available in the EU prior to the AI Act entering into force.