onetrust DataGuidance

SIDLEY

Top 10 Questions on the EU AI Act

E-BOOK | APRIL, 2024

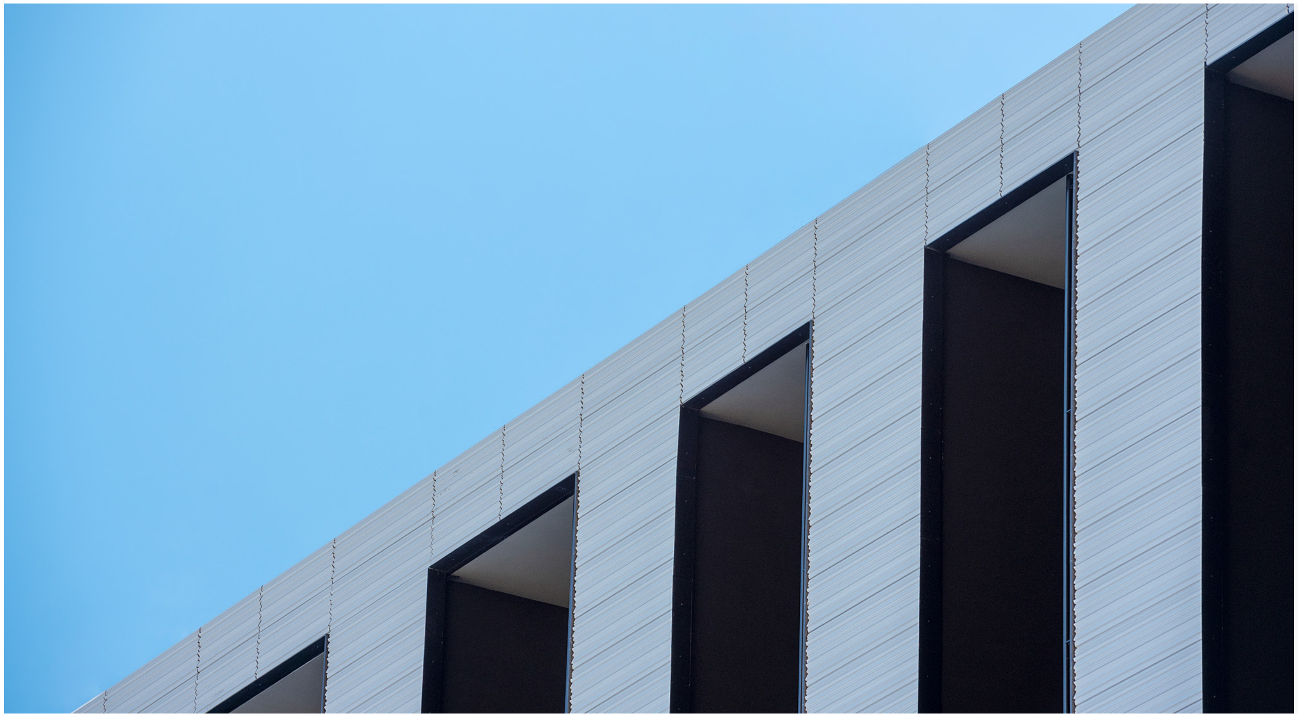
How is an AI system defined?

1. HOW IS AN "AI SYSTEM" DEFINED UNDER THE EU AI ACT AND WHAT DO THE VARIOUS ELEMENTS OF THE DEFINITION MEAN?

An "AI system" has been defined in a rather technical manner in the AI Act as "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."

The key elements of the definition mean, firstly, that an AI system should be "machine-based" i.e., running on machines.

Secondly, a key characteristic, which distinguishes an AI system from traditional software systems or programming approaches, is that it infers information from input data which may include, text, speech, pictures, etc. The system then uses the input data and the instructions or parameters set within it to generate output including predictions (i.e., if X, then Y might happen); content like pictures, graphs, text, etc.; recommendations; or decisions.



Lastly, AI systems under this definition must operate with some degree of autonomy or independence from human involvement and be able to operate without human intervention to a certain degree.

Due to the broad definition of an "AI system," it is likely that many systems that generate decisions, predictions, content, and recommendations will be viewed as an "AI system" under the AI Act but this will require an assessment by organizations of their uses of AI.

Is my organization in scope of the EU AI Act?

2. HOW CAN I KNOW IF MY ORGANIZATION IS IN SCOPE OF THE EU AI ACT? WHAT IF MY ORGANIZATION IS JUST DEVELOPING AI FOR INTERNAL USE/INTERNAL DISTRIBUTION?

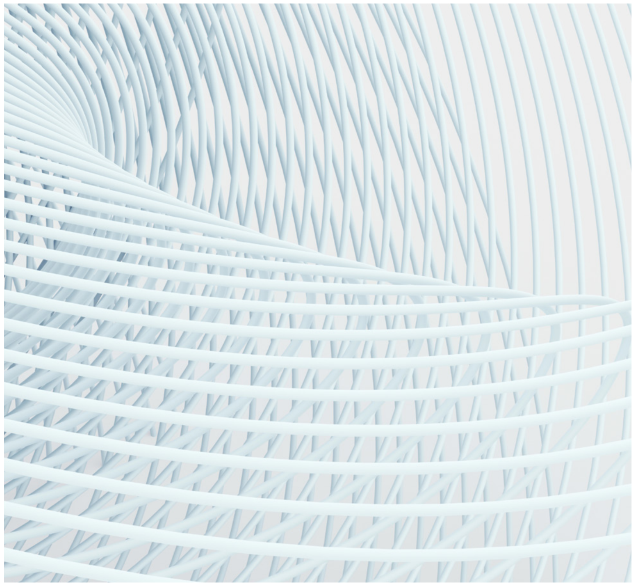
The AI Act will apply to both public and private actors such as companies. It will apply to organizations based inside and outside the EU as long as there is a connection with the EU, i.e., because of the organization's establishment in the EU; because the organization is commercializing, importing, or distributing AI systems in the EU; or because the AI system's output is used in the EU.

The AI Act applies to various actors in the commercial value chain, including "product manufacturers" (the organization that places on the market or puts into service an AI system together with its product and under its own name or trademark), "providers" (the organization that puts into service or places an AI system on the EU market under its own name or trademark), "distributors," "importers," and "deployers" (or users) of AI systems.

An organization that develops its own AI systems and solely uses or offers them internally, is not manufacturer/provider within the meaning of the AI Act because this concept requires a commercial offering of the AI system on the EU market. However, such an organization could still qualify as a deployer (or user) of an AI system within the meaning of the AI Act provided its use of the AI system generally falls in scope of the AI Act (e.g., on the basis of the territorial scope of the AI Act).

Certain AI systems are, irrespective of their level of risk, exempted from the scope of the AI Act – these include AI systems used for the sole purpose of scientific research and development (including, where the R&D activity is for development of the AI system itself).

In addition, certain AI systems will not be considered high-risk when – although meeting the Act's high-risk criteria – they are merely used to (i) perform a "narrow procedural task" (e.g. transforming an unstructured into a structured data set), (ii) improve the result of an activity previously completed by a human (e.g., improve the drafting in a document drafted by a human), (iii) detect (deviations from) decision-making patterns in a human assessment (e.g., detect whether a teacher's paper grading patterns are aligned), and (iv) perform preparatory tasks for high-risk use cases (e.g., indexing, text processing, and translation of files used for a high-risk use case). As a result, organizations will need to do a review of their uses of AI to determine if they are in scope of the AI Act and if so whether they qualify as a manufacturer/provider or a deployer.



What are the current risk levels?

3.WHAT ARE THE CURRENT RISK LEVELS UNDER THE AI ACT AND IS THERE A CHECKLIST, FLOW CHART OR SOME OTHER TYPE OF DOCUMENT I CAN USE TO DETERMINE WHAT LEVEL OF RISK MY ORGANIZATION FALLS UNDER?

The AI Act does not regulate any and all AI systems, but takes a risk-based approach whereby the regulatory obligations imposed increase as the presumed risk level posed by the AI system use case increases.

The AI Act's risk-based approach has one of the four following key risk levels: (i) unacceptable risk (which are prohibited from being provided or used in the EU, e.g., AI systems used for social scoring); (ii) high-risk (which are subject to the most onerous regulatory requirements under the Act, e.g., AI systems used in medical devices, AI used on HR recruitment, AI used in critical and digital infrastructure, and AI used in education and vocational training); (iii) limited risk (which are subject to a number of transparency requirements under the Act, e.g., chatbots, and other AI interacting with individuals); and (iv) minimal or no-risk (which are not regulated under the AI Act, e.g., spam filters).

The AI Act also regulates general-purpose AI ("GPAI") models, and distinguishes between GPAI models with and without "systemic risk" – see Question 7 below.

Unfortunately, no official checklist or flow chart has been issued so far by EU authorities to determine what level of risk an organization's (use of) AI may fall under – although, the EU Commission FAQs on the AI Act provide for a summary of the various risk categories. Organizations should consider doing their own independent legal assessments of their AI systems against the various risk levels, on the basis of the AI Act's final compromise text.

The final compromise text of the AI Act emphasizes the responsibility of providers, deployers, and other actors in relation to AI literacy, meaning that they should ensure that their staff and other persons dealing with AI have the necessary skills and knowledge. To this end, it is key for organizations who do not currently have that skillset and knowhow in-house to seek appropriate counsel to guide them in these assessments.

Who is subject to this?

4. WHAT DOES THE FUNDAMENTAL RIGHTS IMPACT ASSESSMENT, REQUIRED UNDER THE EU AI ACT, ENTAIL AND WHO IS SUBJECT TO THIS?

Under the AI Act, a fundamental rights impact assessment (FRIA) is required to be undertaken by deployers that are (i) bodies governed by public law, or (ii) private operators providing public services and private operators deploying high-risk AI systems used to evaluate an individual's creditworthiness/credit score and AI used for life and health insurance risk assessment and pricing.

A FRIA consists of an assessment of the specific risks or harm to individuals against the deployer's processes of human oversight, internal governance, complaint, and other risk remediation measures. Deployers are required to notify the competent market surveillance authority of the results of the FRIA and, where a deployer has already carried out a data protection impact assessment (DPIA) under the GDPR which partly satisfies FRIA requirements, then the FRIA may be conducted in conjunction with that DPIA.

Although, based on the latest text of the AI Act, the mandatory use of a FRIA is limited to certain situations, organizations should consider doing an AI assessment as part of an AI governance program which could include carrying out a DPIA.

5. WHAT DOES MY ORGANIZATION, AS A USER/DEPLOYER OF AI SYSTEMS IN SCOPE OF THE EU AI ACT, NEED TO DO? AND WHAT COULD CAUSE A USER OR DEPLOYER TO BE CONSIDERED A PROVIDER UNDER THE AI ACT?

The obligations imposed on deployers again depend on the specific risk level of the AI system (use case) involved. In relation to prohibited AI system use cases (e.g., those used for social scoring), deployers are prohibited from using ("deploying") these in the EU – i.e., their output cannot be used in the EU.

In relation to high-risk AI systems, a number of specific regulatory obligations apply to deployers including the implementation of human oversight, adequate measures to control and assess the relevance, and adequacy of the AI system's input data in relation to the AI system's intended purpose, measures to monitor the AI system's functioning in line with the provider's instructions of use and notify the provider of any deviations and serious incidents, keep automated record-keeping logs, etc.

Deployers of limited-risk AI (e.g., generative AI that is not otherwise high-risk) are mainly subject to transparency obligations – i.e., they must inform the individual that content was artificially generated or manipulated.

Deployers should be aware that they can be "requalified" as a provider in the following instances: (i) they put their name or trademark on a high-risk AI system already on the EU market, (ii) they make a substantial modification to a high-risk AI system already on the EU market and the AI system continues to fall within a high-risk category, or (iii) they modify the intended purpose of an AI system already on the EU market so that it becomes a high-risk AI system.

As a result, procedures should be considered as part of an AI governance program to avoid a deployer being requalified as a provider, for example checking that the deployer's employees are following instructions of use for AI systems.

How should organizations navigate the act?

6. HOW SHOULD NON-EU BASED ORGANIZATIONS NAVIGATE THE AI ACT?

Organizations established outside the EU may also be subject to the EU AI Act, and should first perform a scoping exercise to determine, in relation to each of their AI system (use cases), whether they (i) provide, import, or distribute any AI systems in the EU (i.e., as a "provider") (e.g., a U.S.-based organization is developing and acting as the provider, importer, or distributor of AI systems in the EU); or (ii) deploy any AI systems which output is then used in the EU (e.g., an AI-based recruitment tool is used by a U.S.-based organization to recruit EU employees).

Then, they should proceed to determine whether any of their AI system (use cases) fall within one or more regulated risk category under the AI Act (i.e., does the AI system (use case) involve an unacceptable, high, or limited level of risk). Finally, they should consider whether they act as a provider, importer, distributor, or deployer for such AI system (use cases), as the regulatory requirements will differ depending on their role in the value chain.

7. HOW DOES THE AI ACT REGULATE GENERATIVE, FOUNDATION AND GENERAL-PURPOSE AI?

The final compromise text of the AI Act no longer distinguishes or regulates AI models on the basis of whether they are qualified as "Foundation" or "Generative" AI (but only adopts the concept of general-purpose AI (GPAI)) models, which essentially are models that are able to competently perform a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications, and which foundation and generative AI models could fall under.

An example of a GPAI model is a large generative AI model that allows for the flexible generation of content (text, audio, or images), and that can accommodate a wide range of tasks for that reason. The AI Act also contains the concept of a GPAI system, which is the AI system based on a GPAI model that has the capability to serve a variety of purposes and can also be integrated into other AI systems or used on a standalone basis.

Providers of GPAI models are subject to a specific set of regulatory obligations under the AI Act, depending on whether they involve systemic risk or not. Under the AI Act, GPAI models that were trained using a cumulative amount of computing power greater than 10^25 floating point operations ("FLOPs") are presumed to involve "systemic risk."

If the GPAI models are not presumed to entail "systemic risk," those providers are subject to requirements including the drawing up of appropriate technical documentation, a copyright policy, and a detailed summary of the content used to train the GPAI model. If they are presumed to entail a systemic risk, additional obligations apply, including to perform model evaluation and adversarial testing, mandatory systemic risk mitigation and serious incident reporting to the AI Office, and national competent authorities where appropriate. Only the GPAI model provider and not the other actors in the ecosystem, e.g., deployers are subject to these specific regulatory obligations applicable to GPAI models.

GPAI system providers or deployers, on the other hand, are not subject to a specific set of obligations under the AI Act – unless the GPAI system also qualifies as an unacceptable, high, or limited risk system.

Who are the competent authorities?

8. WHO ARE THE "COMPETENT AUTHORITIES" UNDER THE AI ACT? WILL THE EU AI ACT BE ADOPTING A "ONE-STOP-SHOP" SYSTEM OR ARE THOSE IN SCOPE POTENTIALLY SUBJECT TO INTERPRETATIONS/ENFORCEMENT BY 27 DIFFERENT EU MS? AND WHAT IS THE EXPECTED GENERAL ENFORCEMENT STRATEGY?

Each Member State must designate at least one notifying authority and one market surveillance authority as national competent authorities for purposes of enforcing the AI Act.

In turn, the AI Act has not adopted a centralized system of enforcement but like the GDPR, had opted for a decentralized enforcement system with enforcement at the EU Member State level (with the exception of GPAI models who are supervised by the AI Office, see below). In addition, unlike the GDPR, the AI Act also does not foresee a "one-stop-shop" mechanism whereby the various competent national authorities are subject to certain cooperation mechanisms (or where a regulatory investigation would be led by a "lead authority").

In addition, the EU Commission will establish a new AI Office, which administratively will sit within the EU Commission, but which will act with full independence from a regulatory enforcement perspective. The AI Office's main task is to supervise GPAI models with systemic risk and develop codes of practice to encourage the proper application of the AI Act by systemic-risk GPAI model providers. The Commission will also establish a scientific panel of independent experts who have specific expertise on AI and which shall advise the AI Office.

The AI Act also establishes an AI Board, which is composed of one representative per EU Member State, and which main task is to ensure the consistent and effective application of the AI Act throughout the EU by providing (non-binding) advice, recommendations, and sharing technical expertise. An advisory forum will also be established to advise and provide technical expertise to the AI Board and Commission.

How should organizations navigate the act?

9. WILL THERE BE IMPLEMENTING REGULATIONS TO CLARIFY SOME OF THE REMAINING AMBIGUITIES?

The AI Act foresees in several instances for the Commission to adopt implementing and delegated acts to clarify some of the remaining ambiguities in the AI Act, including to amend or add exemptions for high-risk AI systems, to amend the high-risk use cases in Annex III, and in relation to post-market monitoring of AI systems.

In addition, the AI Act can be amended by delegated and implementing acts to update the FLOP threshold which determines the GPAI model "systemic risk" threshold. It is also likely that guidance will be published by the AI Board and by national competent authorities. Some AI guidance has already been published, for example the French CNIL's Self-Assessment Guide for AI Systems and its AI How-To-Sheets.

10. WHAT IS THE TRANSITIONAL PERIOD UNDER THE AI ACT?

Following its excepted adoption this Spring 2024, the AI Act shall enter into force on the 20th day following that of its publication in the Official Journal. It will be fully applicable following a graduated approach as follows:

- 6 months after entry into force, Member States shall phase out prohibited systems;
- 12 months: obligations for GPAI governance become applicable;
- 24 months: all rules of the AI Act become applicable, including obligations for high-risk systems defined in Annex III (list of high-risk use cases); and
- 36 months: obligations for high-risk systems defined in Annex II (list of Union harmonization legislation) apply.

Disclaimer: This FAQ was prepared by Sidley Austin LLP on the basis of the AI Act's final compromise text, as published on 26 January 2024 and as approved by the EU Parliament on 13 March 2024. This FAQ has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

Sidley and Sidley Austin refer to Sidley Austin LLP and affiliated partnerships as explained at www.sidley.com/disclaimer.

Attorney Advertising—Sidley Austin LLP is a global law firm. Our addresses and contact information can be found at www.sidley.com/en/locations/offices. Prior results do not guarantee a similar outcome. Photos may include Sidley alumni or other individuals who are not Sidley lawyers. Photos may be stock photography.

For further details from Sidley, please contact:
William Long, Partner, Sidley: wlong@sidley.com;
Francesca Blythe, Partner, Sidley: fblythe@sidley.com;
Lauren Cuyvers, Senior Managing Associate, Sidley:
lcuyvers@sidley.com

onetrust
DataGuidance

About OneTrust DataGuidance™

OneTrust DataGuidance™ is an in-depth and up-to-date privacy and security regulatory research platform powered by more than two decades of global privacy law research. Hundreds of global privacy laws and over ten thousand additional resources are mapped into DataGuidance to give customers in-depth research, information, insight and perspectives on the world's evolving list of global privacy regulations. The database is updated daily by over 40 in-house privacy researchers, along with a network of 800 lawyers across over 300 jurisdictions, and by active input as part of OneTrust's regulatory engagement program.

OneTrust DataGuidance is a part of OneTrust, the #1 most widely used privacy, security, and governance platform used by more than 8,000 customers and powered by 150 awarded patents. OneTrust DataGuidance fuels the intelligence for the OneTrust Athena™ AI and robotic automation engine, and integrates seamlessly with the full OneTrust platform, including OneTrust Privacy Management Software, OneTrust DataDiscovery™, OneTrust DataGovernance™, OneTrust Vendorpedia™, OneTrust GRC, OneTrust Ethics, OneTrust PreferenceChoice™, and OneTrust ESG.

In 2020, OneTrust was named the #1 fastest growing company on the Inc. 500. According to the IDC Worldwide Data Privacy Management Software Market Shares Report, 2020, "OneTrust is leading the market outright and showing no signs of slowing down or stopping." OneTrust has raised a total of $920 million in funding at a $5.3 billion valuation from Insight Partners, Coatue, TCV, SoftBank Vision Fund 2, and Franklin Templeton.

OneTrust's fast-growing team of 2,000 employees is co-headquartered in Atlanta and London with additional offices in Bangalore, Melbourne, Denver, Seattle, San Francisco, New York, São Paulo, Munich, Paris, Hong Kong, and Bangkok.

To learn more, visit DataGuidance.com or connect on LinkedIn.