iapp

ARTICLE SERIES

Top 10 operational impacts of the EU AI Act

FULL SERIES

On 12 July 2024, the final text of the EU AI Act was published in the Official Journal of the European Union. The next step for the AI Act was its entry into force 20 days after publication, with many provisions being phased in and implemented over the coming months.

First proposed in April 2021, the AI Act underwent marathon negotiations, which concluded in a political agreement in December 2023. The final text combines a human-centric approach with a product-safety approach and is designed to establish a harmonized framework for AI regulation across the EU. The AI Act is a world first, setting a global precedent for AI regulation through its risk-based approach.

The act will be hugely important and consequential to the governance of AI in the EU and worldwide. The IAPP launched a ten-part series on the EU AI Act's top operational impacts. Jointly written by leading European legal experts, the series will walk through the AI Act's most important features and requirements, translating its provisions into actionable terms.

The articles in this series focus on the act's scope, subject matter, definitions and key actors; understanding and assessing risk; requirements for high-risk AI systems; requirements for general-purpose AI models; AI assurance, testing, evaluation and oversight; regulatory governance; post-market monitoring, information sharing and enforcement; regulatory implementation and application alongside broader EU digital regulation; and leveraging EU General Data Protection Regulation compliance.

The published text of the EU AI Act is only the beginning. Now in force, the act is undergoing a phased approach to implementation, including further rulemaking and enforcement. Moreover, it did not come into force in a vacuum. While the AI Act is a first for EU regulation specifically targeted at the risks associated with certain AI systems, the EU has a growing digital regulatory framework with many intersections to how AI systems are governed, including via the GDPR, NIS2 Directive, Digital Services Act and Digital Markets Act. On a global level, the AI Act comes as an important addition to an increasingly dynamic regulatory ecosystem.

The IAPP Resource Center hosts a topic page dedicated to the latest developments on the EU AI Act. Additionally, the IAPP has a topic page for AI that is regularly updated with the latest news and resources.

Contents

Published July 2024

Subject matter, definitions, key actors and scope

By Arnav Joshi and Nina Khalfi-Lanoux

The EU AI Act is the result of years of political, legal and technical debate and negotiation. In a field as complex and quickly evolving as AI, this has the potential to complicate operational compliance, particularly when the law inevitably introduces novel interpretational questions. Our understanding of the AI Act's provisions and requirements will be shaped and refined by a series of standards and regulatory guidance expected over the next 18 months. However, with a series of obligations likely to apply well before this period and the lead time required to implement AI governance measures, organizations should already be looking to understand and interpret key concepts.

Why should the AI Act matter to your organization?

The AI Act aims to ensure the development and deployment of AI is safe, trustworthy, transparent and respectful of fundamental rights, while accounting for progress and innovation in this epoch-defining space. It creates harmonized EU rules for placing AI systems on the market, putting them into service and governing their use. The act prohibits certain AI practices outright and places specific obligations on operators of different AI systems and general-purpose AI models.

Like the EU General Data Protection Regulation, the AI Act has a wide territorial reach, impacting operators within and outside the EU. It provides for significant sanctions, including high financial penalties and a strong regulatory enforcement framework. In the years ahead, substantial parts of the AI Act are expected to become the gold standard for global AI regulation, making an early understanding of its requirements critical for organizations everywhere.

Key concepts and definitions

The AI Act includes 68 definitions. While some important definitions are entirely new, other terms like placing on the market, making available on the market, putting into service, substantial modification, intended purpose, importer and distributor are helpfully based on existing EU law, particularly EU product safety regulation. As a starting point, some of the key concepts and definitions organizations will need to understand in detail are:

AI system

The AI Act does not define the term AI but rather defines an AI system as, "a machine-based system designed to operate with varying levels of autonomy, 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."

This definition aligns with the one proposed by the Organisation for Economic Co-operation and Development and should be read cumulatively, considering each element. Under both definitions, an AI system must:

- → Be machine-based.
- → Be designed to operate with varying levels of autonomy.
- → Have the ability to infer how to generate outputs from inputs received for explicit or implicit objectives and make decisions that can influence physical or virtual environments.
- → Exhibit adaptiveness after deployment.

When interpreting this definition from a compliance perspective, it may be helpful to review the definitions of both AI and system independently, as a precursor to the elements above.

The AI Act's recitals on the notion of AI have evolved to prioritize inferences in particular, noting this typically includes machine learning and "logic- and knowledge-based approaches that infer from encoded knowledge or symbolic representation of the task to be solved." Previous versions of the AI Act's text provide additional guidance on what these approaches may include.

Practically, it is expected commonly used and understood techniques of AI, such as deep learning, reinforcement learning and ML, computer vision, natural language processing and neural networks will fall within this definition.

While there may be edge cases for certain automated, rules-based software that may require specific assessment over time, such as some forms of robotic process automation, it is worth noting the AI Act clearly intends to exclude traditional software systems that do not meet the cumulative criteria in the definition. It is also likely intended to be narrower in scope than the concept of automated decision-making under the GDPR, which focuses on decisions made by automated means without human involvement but does not, for example, account for elements such as inference.

It is also important to bear in mind that an AI system is not the same as an AI model, which is not specifically defined under the AI Act. Though indirectly governed, the law clarifies that models are essential components of AI systems, not systems in and of themselves. As such, models should be seen as a critical part of the technical infrastructure required for an AI system to function but would require additional components, like a user interface, to generate usable outputs and collectively qualify as a regulated AI system.

General-purpose AI models

Though AI models are not defined, general-purpose AI models are. This term is used in the AI Act to refer to what may otherwise be understood as generative AI or foundation models. The approach taken to governing general-purpose AI has evolved over time, sometimes leading to heated debate on the impact of regulating one of the newest, most promising forms of AI on innovation in the EU. The final definition adopted considers the key functional characteristics of these models, primarily their generality and capability to perform a wide range of distinct tasks competently.

The AI Act defines a general-purpose AI model as "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 released on the market."

Critiques of this definition include that the threshold for what constitutes a large amount of data, currently set at 1 billion parameters or more, may be too low and outdated considering the current state of the art. Another practical question to consider is what threshold, in the absence of guidance, to set for a wide range of distinctive tasks to be in scope. General-purpose AI models that have not yet been released, i.e., experimental or prototype models, are excluded from these obligations, which will apply only to models placed on the market. Lastly, the AI Act also includes provisions on general purpose AI systems, which are AI systems based on general-purpose AI models.

As discussed above, the AI Act primarily applies directly to AI systems and general-purpose AI models. Although it adopts a risk-based approach, some of the obligations, such as those relating to transparency, can apply across risk-categories of AI systems unless they qualify as one or more of the practices prohibited under the AI Act altogether. Most obligations, and corresponding liabilities, under the AI Act relate to the use of high-risk AI systems, and these themes will be covered in detail further in this series.

Who does the AI Act apply to?

Borrowing from product safety law, the AI Act applies to operators across the AI value chain. These include:

- **Providers.** These are the most heavily regulated operator under the AI Act. To qualify, providers must have developed an AI system or a general-purpose AI model, or had one developed on their behalf. They must also have "placed the AI system on the market" or "put the AI system into service." They may also be in scope if their place of establishment or location is in a third country, but outputs produced by their AI system are used in the EU. Lastly, the AI system or general-purpose AI model must be released in the provider's name or trademark to qualify. Most obligations under the AI Act apply to providers of high-risk AI systems.

- **Deployers.** This term refers to an individual or entity that uses an AI system under its authority, except during a personal, nonprofessional activity. Deployers may be established or located in the EU or, as with providers, in third countries, but they are in scope if outputs produced by their AI systems are used in the EU. In a business-to-consumer context, individual users of AI systems cannot be considered deployers under the AI Act. If deployers are acting on someone else's authority, as processors might under the GDPR for example, they would not qualify as deployers.

- **Importers.** These are neither providers nor deployers, but they are located or established in the EU and place AI systems on the EU market that bear the name or trademark of individuals or entities based in third countries. Importers are the first to make these third-country AI systems available in the EU.

- **Distributors.** These individuals or entities include actors in the AI supply chain, besides providers and importers, that make AI systems available in the EU as a follow-on action, after the AI system is imported and placed on the market.

- **Product manufacturers.** Product manufacturers place AI systems on the market or put them into service together with their own product.

- **Authorized representatives.** Similar to requirements under the GDPR, authorized representatives are located in the EU for providers located outside the EU.

Beyond this list, the AI Act naturally also applies to individuals in the EU, framed as affected persons, from the perspective of having and exercising rights under the law. While a definition for affected persons did not make it to the final text of the AI Act, they should generally be understood as individuals, not only citizens, in the EU who might be subjected to or otherwise affected by AI systems.

When assessing the role your organization may play as an operator under the AI Act, it is important to be mindful that:

- An operator may be considered to hold multiple roles, such as provider and deployer, simultaneously. In these scenarios, they will need fulfil the relevant obligations associated with those roles cumulatively.

- More than one entity may hold the same role simultaneously, e.g., two providers for one AI system.

- As with controller and processor designations under the GDPR, although roles may be assigned and ringfenced contractually, the true determinant of a party's role will be the role they perform in practice.

- An operator other than a provider may be deemed to be a provider in certain circumstances.

What is not in scope?

Traditional software that does not meet the cumulative criteria set out in the AI system definition will not be in the scope of the AI Act.

Additionally, the AI Act:

- → Recognizes the unique nature of free and open-source AI software, exempting it from provisions to encourage innovation and collaboration, subject to certain conditions and exclusions. However, this exemption does not apply to AI systems placed on the market or put into service as high-risk AI systems, prohibited AI systems listed under Article 5 or AI systems that fall within the scope of certain Article 50 transparency requirements.

- → Sets out exclusions by sector, acknowledging certain areas require a different regulatory approach. Notably, AI systems used solely for scientific research and development are excluded from the scope of the AI Act, allowing the academic and scientific community to pursue advancements in AI more flexibly. Similarly, it does not govern AI systems developed or deployed for military, defense or national security purposes.

- → Excludes deployers of AI systems who are natural persons using AI systems for purely personal, nonprofessional activities.

Conclusion

The implications of the AI Act are wide-ranging for both organizations and individuals in the EU and worldwide. As has been widely discussed, the new law takes a risk-based approach to regulating AI, discussed in detail in the next article in this series, and relies on a combination of product-safety regulation and fundamental rights, though several key concepts are new. Given the AI Act's extraterritorial scope and its many inevitable overlaps with the GDPR, product safety, consumer protection, fundamental rights and digital regulation, considered and comprehensive governance and compliance programs will be needed, particularly for organizations that, like AI, operate across borders.

Published July 2024

Understanding and assessing risk

By Eduardo Ustaran and Uzma Chaudhry

A defining feature of the EU AI Act that has stood out since the European Commission's first proposal in 2021 is the now largely favored "risk-based approach." However, this is not the first time the approach has been featured in EU regulation. For example, the EU General Data Protection Regulation requires safeguards to be implemented according to the level of risk associated with data processing activities. Similarly, the AI Act places obligations on operators depending on the risk category of their AI use. The goal is to mitigate the risk of AI while promoting innovation to reap the benefits of this transformative technology.

The reason behind this model of regulation is an implicit acknowledgment that technology, such as AI, can be beneficial or risky depending on its uses. By placing risk regulation central to the new law, legislators have sought to craft a legislation that does not regulate a particular technology but what we make of the technology through its use. This is even more relevant in the context of AI, given its role as an emerging technology that can, and will, be deployed for almost unlimited applications from the very trivial to the existential.

This article provides insights on how risk is defined and addressed in the AI Act and unpacks the risk-based approach through a breakdown of the definitions and classification criteria for each risk category identified under the new law.

Understanding risk

Understanding around risk within the AI Act is established through two significant definitions.

Risk is defined under Article 3(2) of the AI Act as "the combination of the probability of an occurrence of harm and the severity of that harm."

"Product presenting a risk" is mentioned in Article 79 of the AI Act and is defined under Article 3(19) of Regulation (EU) 2019/1020 on market surveillance and product compliance. At its core, the AI Act is aimed at promoting the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety and fundamental rights within the EU.

As such, to the extent that AI is seen as a product, a product presenting a risk under Regulation EU 2019/1020 is defined as one that has "the potential to affect adversely health and safety of persons in general, health and safety in the workplace, protection of consumers, the environment, public security, and other public interests protected by applicable Union harmonisation legislation to a degree which goes beyond that is considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned. This includes duration of use and the product's putting into service, installation, and maintenance requirements.

Assessing risk

Essentially, the AI Act identifies different types of AI, in accordance with the different levels of risk they present, as follows:

- → Prohibited AI systems, which by their nature present an unacceptable level of risk.
- → High-risk AI systems.
- → AI systems with transparency risks.
- → General-purpose AI models.
- → General-purpose AI models with systemic risk.
- → Other types of AI that do not fall within the above categories.

Prohibited AI systems

Although the AI Act does not define this risk category, Article 5 exhaustively lists examples of unacceptable AI practices that can threaten the rights of individuals located in the EU.

Prohibited AI systems include systems that deploy subliminal techniques, social scoring systems, predictive policing based solely on profiling or personal characteristics, systems used for untargeted scraping of facial images from the internet or CCTV footage for creating or expanding facial recognition databases, emotion recognition systems in the workplace and schools, and biometric categorization systems for deducing or inferring protected characteristics.

Although real-time remote biometric identification systems in publicly accessible spaces for law enforcement have also been banned, the AI Act provides exceptions for their use. For example, exemptions will be granted to law enforcement if they are deployed for:

- → Conducting targeted searches for victims of abduction, human trafficking and sexual exploitation and searches for missing persons.
- → Preventing specific, substantial and imminent threats to life or safety of natural persons, or to prevent the threat of a genuine and foreseeable threat of a terrorist attack.
- → Identifying and locating a person suspected of committing a crime for the purpose of conducting a criminal investigation, or prosecuting or executing offenses mentioned in Annex II, such as terrorism, trafficking, sexual exploitation, child pornography, murder or illicit trade, among others.

High-risk AI systems

High-risk AI systems were the original focus of the proposed regulation, and although different types of AI have been included as part of the legislative process, they remain at the core of

the regulatory framework. The AI Act sets forth criteria to identify whether an AI system does or does not classify as high risk. However, at the outset, it is useful to note an AI system will be classified as high risk depending on the specific purpose for which it is used. Therefore, careful assessment and understanding of the relevant use cases is essential to determine whether a given AI system qualifies as high risk.

For an AI system to be classified as high risk under the AI Act, it will either meet both conditions set forth in Article 6(1) or be listed as high risk under Annex III.

According to Article 6(1) if the "system is intended to be used as a safety component of a product, or the AI system itself is a product, covered by the Union harmonisation legislation listed in Annex I" and 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," then it meets the classification criteria of being a high-risk AI system.

Alternatively, if the system does not fall within the criteria set out in Article 6(1), then it may be listed as high risk under Annex III, pursuant to Article 6(2). Use cases mentioned under Annex III include biometric systems; critical infrastructure; education and vocational training; employment, workers management and self-employment; access to enjoyment of essential private and public services and benefits; law enforcement; migration, asylum and border control management; administration of justice and democratic processes.

However, if an AI system is listed under Annex III but meets any of the conditions set forth in Article 6(3), then it will not be considered high risk, provided it is not used to profile people. This includes systems that are intended to:

- → Perform a narrow procedural task.
- → Improve the result of a previously completed human activity.
- → Detect decision-making patterns or deviations from prior decision-making patterns.
- → Perform a preparatory task for an assessment relevant for the use cases listed under Annex III.

AI systems with transparency risks

This category, governed by Article 50 of the AI Act, sets forth obligations for both providers and deployers of certain AI systems. According to the Articles 50(1) and 50(2), which set forth obligations for providers, AI systems with transparency risks include AI systems that interact directly with natural persons and AI systems that generate synthetic audio, image, video or text content.

Additionally, according to Articles 50(3) and 50(4), which set forth obligations for deployers, this category includes emotion recognition systems, biometric categorization systems, AI systems that generate or manipulate images, and audio or video content constituting a deepfake AI system that generates or manipulates text published with the purpose of informing the public on matters of public interest.

Based on the above examples, and according to the interpretative guidance of Recital 132 it appears the specific transparency requirements

capture systems that may or may not raise high risks. If they raise high risks, transparency obligations will have to be fulfilled without prejudice to the transparency obligations listed for high-risk AI systems. However, as the AI Act enters its phased implementation, this also creates significant uncertainties about what should be regarded as low, high or unacceptable risk. This may raise complexities that affect both those who are meant to comply with the law and those who are meant to implement and enforce it.

General-purpose AI models and those with systemic risk

Chapter V of the AI Act lays down a legal framework for two types of general-purpose AI: general-purpose AI models and general-purpose AI models with systemic risk.

It is important to note, while the AI Act provides a legal framework for regulation of AI "systems," Chapter V departs from that approach and lays down a framework for the regulation of general-purpose AI "models."

A general-purpose AI system is defined in the AI Act as a system based on a general-purpose AI model with the capability to serve a variety of purposes that can either be used directly or integrated in other AI systems.

A general-purpose AI model is therefore part of the broader technical architecture that underpins a general-purpose AI system and is defined as an AI model "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." However, this definition does not cover AI models that are used before release on the market for research, development and prototyping activities.

The AI Act also establishes a subset of general-purpose AI with systemic risk, which refers to a general-purpose AI model that "has high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks," or "based on a decision of the Commission, ex officio or following a qualified alert from the scientific panel" has those same high impact capabilities with "regard to the criteria set out in Annex XIII." The AI Act then goes on to say a general-purpose AI model "shall be presumed to have high impact capabilities ... when the cumulative amount of computation used for its training measured in floating point operations is greater than 10^{25}." Crucially, the concept of systemic risk is not assessed by a use case but by the computing power of the relevant AI model.

Conclusion

The AI Act represents the most sophisticated example of the so-called risk-based approach to European regulation. The degree of granularity with which it classifies the various levels of risk potentially created by AI technology is one of its defining factors and is a key contributor to its complexity. As AI technology evolves and the AI Act becomes effective in practice, determining which obligations apply to a specific type of AI will be almost as challenging as deploying the necessary measures for compliance with the act.

Published July 2024

Obligations on providers of high-risk AI systems

By Victoria Hordern and Olivier Proust

Providers of high-risk AI systems will need to know Chapter III of the EU AI Act very well. Sections 2 and 3 of Chapter III set out the requirements a provider must meet when making a high-risk AI system available on the EU market.

One way to categorize these different requirements is dividing them broadly into organizational, documentation, system design and regulatory requirements, while recognizing that certain articles perform dual roles.

Product safety, financial institutions and AI literacy

A different approach is available for products with an AI system that are also subject to the EU harmonization legislation listed in Section A of Annex I. These products are regulated by other EU directives and regulations, e.g., on machinery, safety of toys, lifts, medical devices and in vitro diagnostic medical devices.

In these circumstances, according to Article 8(2), providers "have a choice of integrating, as appropriate, the necessary testing and reporting processes, information and documentation they provide with regard to their product into documentation and procedures that already exist and are required under" the EU harmonization law. This approach is encouraged to ensure consistency, avoid duplication and minimize additional burdens. For instance, a provider of a high-risk AI system can rely on a single set of technical documentation, as permitted under Article 11(2).

Likewise, the AI Act allows for providers that are financial institutions subject to the EU financial services law to avoid duplication in certain instances. The obligation to implement certain aspects of a quality management system under the AI Act can be fulfilled by the provider complying with the rules on internal governance arrangements or processes under EU financial services law, according to Article 17(4).

Under the requirements in Article 4 of Chapter III, a provider of any AI system, whether high risk or not, must ensure sufficient AI literacy within its organization. Staff and "other persons," presumably contractors, etc., who deal with the operation and use of the AI

system are expected to have sufficient skills, knowledge and understanding to make an informed deployment of the AI system, as well as to be aware of the opportunities and risks of AI and the possible harm it can cause. Of course, this does not mean each individual needs to demonstrate the same level of AI literacy — this obligation takes into account the context in which the AI system will be used, who will use it and the affected persons.

Articles 8-22

This section provides an overview of the individual Articles 8-22 of Chapter III of the EU AI Act, which contains the core requirements on high-risk AI providers.

Article 8: Compliance with the requirements

Article 8 indicates high-risk AI systems must comply with the requirements under Section 2.

The heading of Section 2 is "Requirements for high-risk AI system," but it is not immediately obvious who is required to comply with the section's requirements. That becomes clear in Section 3, Article 16(1), which notes the provider of high-risk AI systems must "ensure that their high-risk AI systems are compliant with the requirements set out in Section 2." It is also the case that all the actors have a vested interest in ensuring the high-risk AI system complies with the Section 2 requirements. For instance, an importer is required to ensure the provider has drawn up the technical documentation, required under Article 11, before the high-risk AI system is placed on the market, as set out in Article 23(1)(b).

Additionally, the deployer is dependent on the provider complying with a number of its obligations in order for the deployer to meet its own obligations. For instance, the deployer needs to understand the "instructions for use," which the provider is required to produce under Article 13, and to be able to effectively use the measures the provider designs for human oversight as set out in Article 14. Part 4 in this series will discuss importer and deployer obligations concerning high-risk AI systems.

What are the operational implications?
Providers of high-risk AI systems in the EU must comply with Section 2 requirements. Article 8 acknowledges compliance can take into account the intended purpose of the high-risk AI system as well as the acknowledged state of the art on AI and AI-related technologies.

Article 9: Risk-management systems

Article 9 requires providers to identify and manage risks associated with high-risk AI systems. By its very nature, a high-risk AI system is considered to carry greater risk whether from a product safety or a fundamental rights perspective. It is therefore unsurprising there is a requirement for the provider to establish, implement, document and maintain a risk-management system.

What are the operational implications?
A provider must:

- → Identify the known or reasonably foreseeable risks associated with the AI system.
- → Adopt appropriate and targeted risk management measures in view of the identified risks.
- → Test AI systems to ensure the most appropriate risk-management measures are put in place.

The risk management system is not a one-off exercise that happens just before the AI system is launched on the EU market. It is a "continuous iterative process" that runs throughout the entire life cycle of the AI system. A provider should estimate and evaluate the risks that may emerge when the AI system is used for its intended purpose. It should also evaluate other risks possibly arising in light of data gathered from post-market monitoring, a requirement under Article 72, which is assisted by deployers providing data to the provider. A provider should ensure its contracts with deployers include a provision to require the deployer to provide information about the performance of the AI system to help the provider evaluate its compliance with the requirements in Articles 8–15.

Additionally, a provider should keep an eye out for and anticipate situations in which the AI system they have placed on the market is modified or white labeled by another actor, distributor, importer, deployer or other third party, so the actor becomes a provider of a high-risk AI system. This scenario engages the obligations under Article 25, which set out responsibilities along the AI value chain, including that the initial or original provider is required to closely cooperate with new providers of the AI system. The initial provider is expected to provide the necessary information and technical access, unless the initial provider originally specified that its nonhigh-risk AI system should not be changed into a high-risk AI system. What is stipulated in the contract the provider enters into, and the accompanying documents, will be key to setting limitations on how other actors can use the AI system.

Risk is defined in Article 3(2) of the AI Act as "the combination of the probability of an occurrence of harm and the severity of that harm," which encapsulates a relatively well-understood concept that is found in the International Organization for Standardization's ISO 14971, a risk-management standard for medical devices. The decision to take this approach to defining risk clearly links the concept of risk under the AI Act to the world of product safety and the potential for harm to individuals.

Once the risks are identified, the provider must select risk-management measures designed to address these risks. In selecting these measures, under Article 9(4) the provider must ensure they consider the effects and possible interaction resulting from the combined application of all the Section 2 requirements. With respect to its selection of risk-management measures, under Recital 65, the provider should also be able to "explain the choices made and, when relevant, involve experts and external stakeholders." The measures must be implemented so the AI system's residual risk is considered acceptable as set out under Article 9(5). Additionally, when identifying the most appropriate risk management measures, the provider must ensure:

- → The elimination or reduction of risks as far as technically feasible through design and development of the AI system.
- → Where appropriate, the implementation of adequate mitigation and control measures addressing risks that cannot be eliminated.

→ The provision of information required under Article 13 on transparency and, where appropriate, training to deployers.

A provider must therefore be prepared to provide appropriate training on managing risks to the deployer using its high-risk AI. A provider must also test AI systems to identify the most appropriate and targeted risk-management measures and such testing can, in accordance with Article 60, include testing in real-world conditions. Providers also have an obligation to consider whether the intended purpose of the AI system means the system is likely to have an adverse impact on those under 18 years of age or other vulnerable groups, i.e., whether children or vulnerable groups are likely to be exposed to the AI system's operating environment and therefore could be affected.

Article 10: Data and data governance

Datasets are central to operating an AI system. Article 10 requires the provider to implement data governance and management practices to ensure those datasets are appropriate. For instance, it specifically permits the use of special category data for bias-detection purposes.

Article 10 is primarily relevant to providers developing high-risk AI systems that make use of techniques involving the training of AI models with data. If the development of the high-risk AI system is not using techniques involving the training of AI models, then the requirements only apply to the testing datasets, according to Article 10(6). The requirements otherwise apply to training, validation and testing datasets.

What are the operational implications?

The management practices a provider must implement include, among others:

→ Information about how the data was collected and the origin of the data. For personal data this means the original purpose of data collection.

→ Relevant data-preparation processing operations, e.g., annotation, labeling and cleaning.

→ Examination of possible biases likely to affect the health and safety of individuals, have a negative impact on fundamental rights or lead to discrimination that is prohibited.

→ Appropriate measures to detect, prevent and mitigate possible biases identified.

→ Identification of relevant data gaps or shortcomings that prevent compliance with the AI Act and how those gaps or shortcomings can be addressed.

A provider must also ensure all three types of datasets — training, validation and testing — are relevant, sufficiently representative and, as far as possible, free of errors and complete given the intended purpose. The datasets must also have the appropriate statistical properties and must account for the characteristics or elements that are particular to the specific geographical, contextual, behavioural or functional settings in which the AI system is intended to be used by deployers. Note, while a provider should be able to delineate the intended purpose of an AI system, it may not be able to anticipate all the various settings within which a deployer could use the AI system.

Article 10 specifically permits the processing of special category personal data as necessary to

ensure bias detection and correction. However, in addition to complying with the EU General Data Protection Regulation, a provider must also meet additional conditions to use special category personal data for this purpose. These include:

- → Demonstrating the use of other data, including synthetic data or anonymized data, is not sufficient to detect and correct bias.
- → Ensuring the special category data is subject to strict controls on access and only authorised people have access to the data.
- → Ensuring the data is not processed by other parties — although, as an observation, a strict interpretation of this requirement could mean a provider could not use third-party processors for this part of its AI governance framework.
- → Ensuring the special category data is deleted once the bias has been corrected or the data reaches the end of its retention period.

Article 11: Technical documentation

Meeting the obligations under Article 11 will likely require a fair amount of effort for providers. Article 11 requires a description, detailed in places, of technical aspects associated with the AI system, such as system architecture, training methodologies and cybersecurity measures. A provider must create this documentation before a high-risk AI system is placed on the market or put into service and keep it up to date.

What are the operational implications?
Since the main audience of the technical documentation are the national competent authorities and notified bodies, it must be prepared in a clear and comprehensive form. The technical documentation must show how the AI system complies with Section 2 requirements, but it must also, at a minimum, reflect the requirements set out in Annex IV. These are fairly extensive and include the following:

- → A general description of the AI system.
- → A detailed description of the AI system's elements and the process for its development.
- → Information about the monitoring, functioning and control of the AI system.
- → A description of the appropriateness of performance metrics for the specific AI system.
- → A detailed description of the risk-management system.
- → A description of relevant changes made by the provider to the system through its life cycle.

Small and medium-sized enterprises may provide the elements set out in Annex IV in a simplified manner, and the European Commission is required to establish simplified documents.

Article 12: Record keeping

Given the importance of being able to trace automated actions by a high-risk AI system, especially if the operation of the system

caused harm, but also to ensure the AI system functions in accordance with its intended purpose, under Article 12, a provider must design the AI system so it automatically records or logs events during its lifetime. See Article 19 for the corresponding retention periods for these logs.

What are the operational implications?
The AI system should be designed to record relevant events to identify situations that may result in the AI system being a "product presenting a risk" or involving a "substantial modification." These two scenarios essentially are designed to flag harm to individuals and significant changes to the AI system.

In Article 3(19) of the Market Surveillance Regulation 2019/1020, a product presenting a risk is defined as a product that has the potential to negatively affect individuals, "the environment, public security and other public interests, protected by the applicable Union harmonisation legislation, to a degree which goes beyond that considered reasonable and acceptable in relation to its intended purpose or under the normal or reasonably foreseeable conditions of use of the product concerned."

A substantial modification is defined in Article 3(23) of the AI Act and means a change to an AI system after it is placed on the market, which is not foreseen or planned in the initial conformity assessment carried out by the provider, so that compliance with Section 2 of Chapter III is affected or results in a change to the intended purpose of the AI system.

Additionally, the AI system should be designed to record events that facilitate the post-market monitoring system required under Article 72. The AI system should also be designed to record events that are relevant for monitoring the operation of high-risk AI systems referred to in Article 26(5), which refers to AI systems used by deployers.

If a provider has developed an AI system for remote biometric identification, "the logging capabilities shall provide, at a minimum:

a. recording of the period of each use of the system (state date and time and end date and time of each use);

b. the reference database against which input data has been checked by the system;

c. the input data for which the search led to a match;

d. the identification of the individual involved in the verification of the results, as referred to in Article 14(5)."

Article 13: Transparency and provision of information to deployers

Article 13 is not concerned with transparency to individuals affected by the high-risk AI system that is covered by the GDPR when personal data is relevant. Instead, these requirements for providers are to ensure the AI system is developed so that it is sufficiently transparent for deployers. The operation of the AI system must enable deployers to interpret the system's output and use it appropriately. In particular, the design of the AI system must enable both the provider and deployer to comply with their obligations under Section 3.

What are the operational implications?
The provider must ensure its AI system is accompanied by concise, complete, correct and clear instructions for use so that it is relevant, accessible and comprehensive to deployers. The instructions for use must contain certain information, including:

- → The identity and contact details of the provider and any authorized representative.
- → The characteristics, capabilities and limitations of the performance of the high-risk AI system.
- → Human oversight measures, referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the output of the high-risk AI systems by deployers.
- → Details on the computational and hardware resources that deployers need to operate the AI system, its expected lifetime and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of the AI system, including software updates.
- → Where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs, as set out in Article 12.

Article 14: Human oversight

Unsurprisingly, the requirement for human oversight of high-risk AI systems is a core requirement. Under Article 14(1), providers must design and develop high-risk AI systems so they can be effectively overseen by an individual.

The purpose of human oversight indicated by Article 14(2) is to prevent or minimize the risks to health, safety or fundamental rights that may emerge from the use of the AI system.

What are the operational implications?
The human oversight measures the provider implements in the AI system must be commensurate with the risks, autonomy and context of use for the AI system. Human oversight "shall be ensured through either one or both of the following types of measures:

a. measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service; or

b. measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer."

The provider must deliver the AI system to the deployer so that those entrusted with human oversight can carry out certain activities, including:

- → Understanding the relevant capacities and limitations of the high-risk AI system and duly monitoring its operation, including detecting and addressing anomalies, dysfunctions and unexpected performance.
- → Maintaining an awareness of the possibility of automation bias.
- → Correctly interpreting the high-risk AI system's output and considering the available interpretation tools and methods.

Remote biometric identification systems are subject to additional human oversight requirements given the significance of identifying an individual in this context.

Article 15: Accuracy, robustness and cybersecurity

Under Article 15, a provider must design and develop the high-risk AI system so it achieves an appropriate level of accuracy, robustness and cybersecurity, and it performs consistently in those respects throughout its life cycle.

What are the operational implications?

A provider must be able to measure levels of accuracy, although help may come from the European Commission, which shall encourage the development of benchmarks and measurement methodologies. Under Article 13, providers must ensure the instructions of use they provide to deployers include the levels of accuracy and relevant accuracy metrics of AI systems.

Under Article 15, providers must ensure AI systems are "as resilient as possible regarding errors, faults or inconsistencies that may occur within the system or the environment in which the system operates, in particular due to their interaction with natural persons or other systems." Further, AI systems "that continue to learn after being placed on the market or put into service shall be developed in such a way as to eliminate or reduce as far as possible the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures."

Article 15 calls out certain cyber threats to AI systems such as data poisoning, model poisoning and adversarial examples. High-risk AI systems must be resilient against attempts by unauthorized third parties to alter their use, outputs or performance by exploiting system vulnerabilities.

Article 16: Other obligations on providers of high-risk AI systems

Article 16 signals the beginning of Chapter III, Section 3, "Obligations of providers and deployers of high-risk AI systems and other parties." Article 16 identifies all the requirements for providers under Section 2, as well as additional obligations on providers such as the need to affix a CE marking, which denotes European Conformity, to the AI system and registration of the AI system in the EU database.

Certain obligations are not referred to explicitly in Chapter III but fall under the scope of Article 16. The provider will:

- → Ensure the provider's name, registered trade name or trademark, and address are indicated on the high-risk AI system or its packaging or documentation.
- → Ensure the AI system undergoes the relevant conformity assessment as required by Article 43.
- → Prepare an EU declaration of conformity as set out in Article 47.
- → Affix the CE marking to the AI system and its packaging or documentation, according to Article 48.
- → Register the AI system in the EU database when applicable, as set out in Article 49. This only applies to Annex III high-risk AI systems.

→ Ensure the AI system complies with EU accessibility requirements.

What are the operational implications?
Article 16 lays out a useful checklist for providers of high-risk AI systems to understand their obligations, although it does not list out the Section 2 obligations in full and goes beyond Chapter III. A number of the obligations are proactive and must be achieved before placing the AI system on the market, whereas other obligations relate to the ongoing operation of the AI system or are reactive to events.

Article 17: Quality-management system

Article 17 is similar to the accountability requirement under the GDPR. The quality-management system must show how the provider complies with the AI Act through written policies, procedures and instructions.

What are the operational implications?
The QMS document must include certain baseline requirements proportionate to the size of the provider's organization. These include:

→ A strategy for regulatory compliance.

→ Techniques, procedures and systematic actions to be used for the design, design control and design verification of the AI system.

→ Techniques, procedures and systematic actions to be used for the development, quality control and quality assurance of the AI system.

→ Examination, test and validation procedures to be carried out before, during and after development of the AI system, and the frequency with which they have to be carried out.

→ Technical specifications, including safeguards, to be applied.

→ The creation, implementation and maintenance of a post-market monitoring system, i.e., to collect, document and analyze data provided by deployers or collected through other sources on the performance of the high-risk AI system throughout its lifetime.

→ Providers must document their QMS in a way that reflects the high-risk AI system and their organization.

Article 18: Documentation keeping

Article 18 requires the provider to retain certain key documents about the AI system for 10 years in case the national authorities want to see them.

What are the operational implications?
A provider needs to have a secure repository to keep the relevant documentation, including technical documentation, QMS and EU declaration of conformity. They should be ready to provide this to the national authorities.

Article 19: Automatically generated logs

Article 19 requires the provider to retain logs automatically generated by the AI system for at least six months.

What are the operational implications?
The provider needs to implement a mechanism for storing logs, which can be easily accessed by date or time. It must also ensure it has considered the appropriate retention period

for the logs generated, especially those that contain personal data.

Article 20: Corrective actions and duty of information

Under Article 20, if a provider considers that a high-risk AI system it has already placed on the market or put into service does not conform with the AI Act, it must immediately take the necessary corrective action to bring it into conformity or withdraw, disable or recall it, as appropriate.

What are the operational implications?

A provider needs to know how the AI system it is responsible for is being used. The provider should be able to obtain this awareness through implementing the post-market monitoring system mentioned under Articles 17 and 72.

If the provider learns the AI system is not in conformity, it must inform the distributors and, where applicable, the deployers, importers and authorized representative of the nonconforming AI system. Additionally, if there is a product-liability-related risk as set out under Article 79, it must immediately investigate the cause and, where applicable, inform the market surveillance authority and notified body.

Article 21: Cooperation with competent authorities

Providers must provide relevant information to the authorities on request and give them access to the logs referred to in Article 12.

What are the operational implications?

Providers should ensure their personnel can recognize a request from an authority by providing relevant training and awareness. Once a request is received from an authority, the provider must respond promptly.

Article 22: Authorized representatives of providers of high-risk AI systems

Article 22 requires providers not established in the EU to appoint an authorized representative in the EU under a mandate.

What are the operational implications?

The mandate between the provider and representative must empower the representative to carry out certain tasks verifying the EU declaration of conformity and technical documentation for the AI system, to keep documents and information for the competent authorities for 10 years after the AI system is placed on the market, and to cooperate with the authorities. A representative may also terminate the mandate if it has reason to believe the provider is acting contrary to its obligations under the AI Act.

Annex

Articles 8-15 comprise Section 2 of Chapter III and Articles 16-27 make up Section 3. If we treat Articles 8-22 as containing the core requirements on high-risk AI providers, it is possible to break down the requirements as set out in the following table. Please note our assessment of the obligations for the use of high-risk AI systems by other actors who are not providers will follow in Part IV of this series.

	LINKS WITH	REQUIREMENT
Article 8: Compliance with the requirements	Section 2	Organizational process
Article 9: Risk-management system	Articles 72, 13 and 60	Documentation and system design
Article 10: Data and data governance	None	System design
Article 11: Technical documentation	Annex IV	Documentation
Article 12: Record keeping	Articles 79, 72 and 26	Documentation and system design
Article 13: Transparency and provision of information to deployers	Articles 12, 14 and 15	System design
Article 14: Human oversight	Annex III	System design
Article 15: Accuracy, robustness and cybersecurity	None	System design
Article 16: Obligations of providers of high-risk AI systems	All of Section 2 of Chapter III, Articles 17-20, Articles 43, 47-49	Organizational, documentation, system design and regulatory
Article 17: Quality-management systems	Articles 9, 72 and 73	Documentation
Article 18: Document keeping	Articles 11, 17 and 47	Documentation
Article 19: Automatically generated logs	Article 12	Documentation
Article 20: Corrective actions and duty of information	Article 79	Regulatory
Article 21: Cooperation with competent authorities	Article 12	Regulatory
Article 22: Authorized representatives	Section 2, Articles 47 and 49	Regulatory

Published August 2024

Obligations on nonproviders of high-risk AI systems

By Olivier Proust and Victoria Hordern

What should you do if you are using or handling a high-risk AI system but are not a provider? The AI Act imposes a comprehensive set of obligations on deployers, importers, distributors and authorized representatives to ensure the safe and compliant use of high-risk AI systems within the EU.

These stakeholders must work together to uphold the principles of transparency, safety and accountability to foster trust and innovation in the AI ecosystem. Through diligent adherence to these regulations, the potential risks associated with AI can be mitigated, ensuring the benefits of AI are realized while protecting the fundamental rights and safety of individuals. The obligations imposed on deployers, importers, distributors and authorized representatives appear in Chapter II, Section 3.

Obligations of deployers

Deployers have a general obligation to take appropriate technical and organizational measures to ensure they are using high-risk AI systems in accordance with the instructions for use accompanying such systems. Deployers may be subject to further obligations under EU or national law in addition to those in the AI Act.

AI literacy

Although Article 4 does not appear in Chapter II, Section 2, it does appear at the end of Chapter I and imposes an obligation on deployers to ensure their staff and others dealing with the operation and use of AI systems have sufficient AI literacy. Deployers should consider the technical knowledge, experience, education and training; the context of how the AI systems will be used; and the people using them.

Under Article 3, the objective of AI literacy is to enable deployers and other parties to make informed decisions about AI systems and their deployment, as well as to gain awareness about the opportunities, risks and possible harms AI can cause. These notions may vary depending on the context the AI is used in, which suggests deployers must adapt their training to be meaningful for their staff, so the staff can acquire the necessary skills and knowledge about the AI being deployed.

For deployers, AI literacy may include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use or the suitable ways to interpret the AI system's output.

The EU AI Board is required to support the European Commission in promoting AI literacy tools, as well as public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems.

Due diligence

Deployers are generally not subject to due diligence requirements, unlike importers and distributors of high-risk AI systems.

However, deployers that are public authorities and EU institutions, bodies, offices or agencies must first verify the high-risk AI system they intend to use has been properly registered in the EU database in accordance with Article 49. They must also refrain from using an AI system that has not been registered.

Compliance and monitoring

Deployers are required to monitor the operation of the high-risk AI system based on the instructions for use they receive from the provider. When relevant, they must give feedback to the provider, which enables the provider to comply with the system's post-market monitoring obligations.

If the deployer has any reason to believe use of the high-risk AI system in accordance with the instructions for use may result in it presenting a risk to the health, safety and fundamental rights of individuals, see Article 79(1), the deployer must inform the provider or distributor and the relevant market surveillance authority without undue delay and suspend further use of that system.

Financial institutions that are deployers are deemed to have fulfilled their monitoring obligation if they have complied with the rules under EU law on internal governance arrangements, processes and mechanisms that apply to the financial sector.

When Article 35 of the EU General Data Protection Regulation requires deployers to carry out data protection impact assessments, they may rely on the instructions for use given by the provider for assistance.

Human oversight

Deployers must assign human oversight to natural persons who have the necessary competence, training, authority and support to oversee the use of high-risk AI systems. Deployers remain free to organize their own resources and activities to implement the human oversight measures indicated by the providers.

To the extent the deployer exercises control over the input data, it must ensure the input data is relevant and sufficiently representative of the high-risk AI system's intended purpose.

Incident reporting

If a deployer has identified a serious incident, it must immediately inform the provider, then the importer or distributor and the relevant market surveillance authorities.

Transparency and information

Before "putting to service" or using a high-risk AI system in the workplace, deployers who are

employers must inform affected workers and their representatives that they will be subject to the use of the high-risk system, in accordance with the rules and procedures under EU or national law.

Regardless of the transparency requirements that apply to certain AI systems, such as chatbots, generative AI, deepfakes or emotion-recognition systems, deployers of high-risk AI systems referred to in Annex III, those concerned with fundamental rights rather than product safety, that make or assist in making decisions related to natural persons must inform them about the use of the high-risk AI system.

Recordkeeping

When a high-risk AI system processes personal data, deployers must keep the automatically generated logs for a period appropriate to the system's intended purpose, which is at least six months, unless indicated otherwise in applicable EU or national law, particularly the GDPR.

Financial institutions that are deployers must maintain the logs as part of the documentation they are required to keep in accordance with EU laws applicable to the financial sector.

Cooperation with the authorities

Deployers must cooperate with the relevant competent authorities in any action they take regarding the high-risk AI system to implement the AI Act. Deployers of post-remote biometric identification systems must also submit annual reports to the relevant market surveillance and data protection authorities. Specific additional obligations apply to deployers of post-remote biometric identification systems.

Fundamental rights impact assessment

Article 27 of the AI Act mandates deployers of high-risk AI systems to conduct fundamental rights impact assessments to evaluate and mitigate potential adverse impacts on fundamental rights. However, unlike data protection impact assessments imposed on any controller of a high-risk processing activity, FRIAs are limited to certain high-risk AI systems and some deployers. Significantly, providers are not required to carry out FRIAs because deployers decide to use AI systems for specific concrete purposes.

FRIAs only apply to high-risk AI systems that fall under Article 6.2 of the AI Act. Deployers of high-risk AI systems that are intended to be used as safety components of products or are products themselves, covered by the EU harmonization legislation and pursuant to Article 6.1 of the AI Act, are not required to carry out FRIAs. High-risk AI systems that fall under Article 6.1 are already required to undergo third-party conformity assessments before they are placed on the market or put into use.

Furthermore, deployers of high-risk AI systems that are intended to be used as safety components in the management and operation of critical digital infrastructure or road traffic or in the supply of water, gas, heat or electricity are also excluded from the obligation to carry out FRIAs.

For all other high-risk AI systems that fall under Annex III, the obligation to carry out FRIAs is limited to the following categories of deployers:

- → Public law entities.
- → Private operators that provide public services, such as education, health care,

social services, housing and administration of services.

- Other private operators, such as banks and insurance entities, that deploy AI systems to evaluate creditworthiness, establish a credit score, and assess risk and pricing for life and health insurance.

This means, in practice, many deployers using high-risk AI systems will not be required to perform FRIAs though they may still need to carry out DPIAs.

FRIAs must contain the following information:

- A description of the deployer's processes that will use the high-risk AI system in line with its intended purpose.
- A description of the period in which and the frequency with which each high-risk AI system is intended to be used.
- The categories of natural persons and groups likely to be affected by the system's use in the specific context.
- The specific risks of harm likely to impact the categories of persons or groups of persons identified pursuant to the last bullet above, taking into account the information given by the provider pursuant to Article 13, i.e., instructions for use.
- A description of the implementation of human oversight measures, according to the instructions for use.
- The measures to be taken when those risks materialize, including the arrangements for internal governance and complaint mechanisms.

Deployers are only required to carry out FRIAs for the first use of a high-risk AI system. They may rely on previously conducted FRIAs or existing impact assessments carried out by the provider. They may also rely on DPIAs if one has been carried out that reflects the FRIA's obligations. Deployers have an obligation to keep their FRIAs up to date. Once the assessment has been performed, deployers must notify the market surveillance authority of the results. This will involve submitting a completed template questionnaire developed by the AI Office.

By performing this assessment, deployers ensure their use of high-risk AI systems is compliant with legal standards and aligned with the broader ethical obligations to protect and promote fundamental human rights, thereby fostering greater public trust and acceptance of AI technologies.

Obligations of importers

Importers that place high-risk AI systems on the EU market are subject to rigorous checks to ensure compliance with the AI Act. See the table below for a comparison of the obligations of importers and distributors.

Due diligence

Before importers place high-risk AI systems on the market, they must verify the AI system's conformity with the AI Act. In particular, they must verify:

- The provider has conducted the proper conformity assessment in accordance with Article 43.

- → The provider has drawn up the technical documentation of the AI system.
- → The AI system bears the required CE marking and is accompanied by the EU declaration of conformity and instructions for use.
- → The provider has appointed an authorized representative in accordance with Article 22(1), when required.

Compliance

Importers must indicate their name, registered trade name or registered trademark, and the address where they can be contacted on the high-risk AI system and its packaging or accompanying documentation, when applicable. While a high-risk AI system is under their responsibility, they should ensure the storage or transport conditions do not jeopardize the system's compliance with the requirements under Chapter III, Section 2 of the AI Act.

Importers should not place a high-risk AI system on the market if there is reason to believe it does not conform with the AI Act, is falsified or is accompanied by falsified documentation until the system has been brought into conformity. Presumably, the provider must bring the high-risk AI system into conformity, given that the importer is required in such cases to inform the provider about the risks of the AI system.

Documentation and recordkeeping

Importers must keep a copy of the EU declaration of conformity, the certificate issued by the notifying body and the instructions of use for 10 years after the high-risk AI system is placed on the market or put into service. Importers must also ensure technical documentation is available for regulatory authorities upon request.

Reporting

Importers must inform the provider of the high-risk AI system, the authorized representative and market surveillance authorities when it presents a risk to the health, safety or fundamental rights of persons within the meaning of Article 79(1).

Cooperation with authorities

Importers are obligated to provide the relevant competent authorities with all necessary information and documentation related to the AI system, including technical information, upon reasoned request. They must also cooperate with relevant competent authorities on any action they take regarding a high-risk AI system the importers placed on the market to reduce and mitigate the risks it poses.

Obligations of distributors

Distributors that make high-risk AI systems available on the EU market must ensure these systems comply with the AI Act's requirements. A number of these obligations are similar, but not identical, to those of the importers. See the table on Page 34 for a comparison of the obligations of importers and distributors.

Due dilligence

Before making a high-risk AI system available on the market, distributors are required to verify that the system conforms with the AI Act. Distributors must verify that AI systems bear the CE marking and are accompanied by a copy of the EU declaration of conformity and instructions of use. They also need to ensure providers and importers have complied

with their respective obligations, including conformity assessments.

Compliance

While a high-risk AI system is under their responsibility, distributors must ensure the storage or transport conditions applied to such AI do not jeopardize their compliance with the requirements under Section 2, Chapter III of the AI Act.

Furthermore, based on the information in its possession, when a distributor believes a high-risk AI system does not comply with the requirements, it must not make the system available on the market until it complies. Presumably, the provider of the AI system will ensure compliance.

If the system has already been placed on the market, the distributor must take any corrective action needed to bring it into compliance, withdraw it, recall it or ensure the provider, importer or relevant operator takes corrective actions.

Reporting

When a distributor believes a high-risk AI system that does not comply with Section 2, Chapter III of the AI Act presents a risk to the health, safety or fundamental rights of persons within the meaning of Article 79(1), it must inform the provider or the importer of the AI system before it is placed on the market. If the AI system has already been placed on the market, the distributor must immediately inform the provider or importer of the AI system and the relevant competent authorities of the member states, providing the details of noncompliance and any corrective actions taken.

Cooperation with the authorities

Distributors must provide the relevant competent authorities with all necessary information and documentation regarding the distributor's actions to demonstrate the system's conformity with Chapter III, Section 2 of the AI Act, upon reasoned request. Distributors must cooperate with relevant competent authorities in actions regarding the high-risk AI systems they have made available on the market, in particular to reduce and mitigate their risks.

Obligations of authorized representatives

The roles and obligations of authorized representatives are directly linked to providers. Providers that are established in third countries outside the EU are required to appoint authorized representatives in the EU prior to making their high-risk AI systems available on the EU market.

Authorized representatives can be any natural or legal person located or established in the EU who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to respectively perform and carry out the obligations and procedures established by the AI Act on behalf of the provider.

Mandate and documentation

Authorized representatives must hold a written mandate from the provider specifying their tasks and responsibilities. They must also provide a copy of the mandate to market surveillance authorities upon request.

Pursuant to this mandate, the authorized representative is required to carry out the following tasks based on the steps below.

Due diligence

The authorized representative must verify the EU declaration of conformity, the technical documentation referred to in Article 11, has been drawn up and the provider has carried out an appropriate conformity assessment procedure. Further, when a provider has registered a high-risk AI system in the EU database referred to in Articles 49 and 71, the authorized representative must verify that the information referred to in Point 3 of Section A of Annex VIII is correct.

Compliance

Authorized representatives are obligated to terminate the mandate with a provider if they believe or have reason to believe the provider is acting contrary to its obligations pursuant to the AI Act. When applicable, the authorized representative must register the high-risk AI system in the EU database, per Articles 49 and 71, unless the provider has already done so.

Recordkeeping

The authorized representative must keep the provider's contact details, a copy of the EU declaration of conformity, the technical documentation and the certificate issued by the notified body, when applicable, for 10 years after the high-risk AI system is placed on the market or put into service.

Reporting

When the authorized representative decides to terminate the mandate with a provider, it must immediately inform the relevant market surveillance authority and the notified body, when applicable, including its reasons for doing so.

Cooperation with the competent authorities

The authorized representative must act as the point of contact for national authorities within the EU. They must provide the competent authorities with documentation and information necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Chapter III, Section 2 of the AI Act, including access to the logs, upon reasoned request. Also upon reasoned request, the authorized representative must cooperate with competent authorities on any action they may take about the high-risk AI system, in particular, to reduce and mitigate the risks it poses.

Responsibilities along the AI value chain

Article 25 of the AI Act considers situations in which a deployer, importer, distributor or third party of a high-risk AI system becomes a provider when specific actions are taken.

Indeed, any distributor, importer, deployer or other third party shall be considered a provider of a high-risk AI system and shall be subject to the obligations of the provider under Article 16 if:

- → They put their name or trademark on a high-risk AI system that has already been placed on the market or put into service, regardless of the contractual arrangements between the parties.

- → They make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system under Article 6.

→ They modify the intended purpose of an AI system, including general-purpose AI systems, which was not classified as high-risk when it was placed on the market or put into service but became a high-risk AI system as a result of modification.

Under the AI Act, if a deployer, importer or distributor takes any of the above actions, the provider that initially put the high-risk AI system on the market or into service is no longer considered a provider of that specific AI system. Therefore, depending on the situation, there is a change of designated role and a shift of responsibility from the initial provider to the new provider, which was previously a deployer, importer or distributor.

Nonetheless, the initial provider must closely cooperate with any new providers, make the necessary information available and provide the reasonably expected technical access and other assistance required to enable the new providers to fulfil their obligations, especially regarding compliance with the conformity assessment of high-risk AI systems.

However, in its contract with a deployer, importer or distributor, the initial provider can stipulate that its AI system is not to be changed into a high-risk AI system. In those cases, the initial provider has no obligation to hand over the documentation. Presumably, this only applies to AI systems that are not classified as high-risk when they are initially placed on the market or put into service.

For high-risk AI systems that are safety components of products, product manufacturers are considered providers and, therefore, must comply with the obligations imposed on providers under Article 16 when either the high-risk AI system is placed on the market with the product under the name or trademark of the product manufacturer or the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

Finally, any third party that supplies an AI system or tools, services, components or processes used or integrated with a high-risk AI system must enter into a written agreement with the provider. The agreement should specify the necessary information, capabilities, technical access and other assistance based on the generally acknowledged state of the art to enable the provider of the high-risk AI system to fully comply with its obligations under the AI Act. This requirement does not apply to third parties that make tools, services, processes or components accessible to the public under a free and open license, except general-purpose AI models.

The AI Office may develop and recommend voluntary model terms for contracts between providers of high-risk AI systems and third parties similar to the standard contractual clauses between controllers and processors under the GDPR.

Comparison of importer and distributor obligations

	IMPORTERS	DISTRIBUTORS
Due diligence	Verify that the provider has: → Conducted the proper conformity assessment in accordance with Article 43. → Drawn up the technical documentation of the AI system. → Appointed an authorized representative in accordance with Article 22(1), when required. Verify that the AI system has the required CE marking and is accompanied by the EU declaration of conformity and instructions for use.	Verify that providers and importers have fulfilled their obligations, including conformity assessments. Verify that AI systems bear the CE marking and are accompanied by a copy of the EU declaration of conformity and instructions for use.
Compliance	Indicate their name, registered trade name or registered trademark, and address on the AI packaging or its accompanying documentation. Ensure the storage or transport of AI does not jeopardize the AI system's compliance with Section 2, Chapter III of the AI Act. Not place any AI system that is noncompliant, falsified or accompanied by falsified documentation on the market until it has been brought into conformity.	Ensure the storage or transport of AI does not jeopardize the AI system's compliance with Section 2, Chapter III of the AI Act. Not make any noncompliant AI system available on the market until it has been brought into conformity. When a noncompliant AI system has been made available on the market, take the corrective actions necessary to bring it into conformity, withdraw it, recall it or ensure the provider, importer or any relevant operator takes those corrective actions as appropriate.
Recordkeeping	Keep a copy of the EU declaration of conformity, the certificate issued by the notifying body and the instructions of use for 10 years after the high-risk AI system is placed on the market or put into service. Ensure technical documentation is available for regulatory authorities upon request.	N/A
Reporting	Inform the provider of an AI system, the authorized representatives and the market surveillance authorities, but not the deployer, of any risks posed by such AI system.	Inform the provider or the importer of an AI system of any risks, as defined under Article 79(1), posed by such AI system. Immediately inform the provider or importer and the competent authorities when it has made an AI system that presents a risk, as defined under article 79(1), available on the market and that AI system does not comply with Section 2, Chapter III of the AI Act. This includes providing the details of noncompliance and any corrective actions taken.
Cooperation with the authorities	Provide the authorities with all necessary information and documentation related to the AI system, including technical information, upon reasoned request. Cooperate in any action taken by the authorities in relation to high-risk AI systems.	Provide the authorities with all necessary information and documentation regarding actions taken to demonstrate conformity of an AI system with Section 2, Chapter III of the AI Act, upon reasoned request. Cooperate with any action taken by the authorities in relation to high-risk AI systems made available on the market, in particular to reduce and mitigate the risks it poses.

Published August 2024

Obligations for general-purpose AI models

By Phillip Lee and Uzma Chaudhry

If you were to read the European Commission's original AI Act proposal, published in April 2021, you would find it conspicuously devoid of references to general-purpose AI. With the benefit of hindsight, this might seem like a surprising omission. Yet, outside of the world of AI experts, few people had ever heard of general-purpose AI at the time the proposal was published.

Fast-forward to a little over one year later, OpenAI released ChatGPT to an unsuspecting public in November 2022, wowing them with its human-like, if sometimes unreliable, responses to their prompts. It quickly went viral, reportedly reaching 100 million users in just two months and becoming the fastest adopted consumer app of all time.

As a result, terms like large language models, generative AI and general-purpose AI began to enter the consciousness of European legislators, if not exactly the public consciousness. Clearly, the AI Act would need to regulate general-purpose AI, but how?

This was not an easy question to answer. The proposed law worked by placing AI systems into prohibited, high and low risk buckets to decide which rules to apply. However, by its very nature, general-purpose AI could be implemented across an unimaginably wide range of use cases that spanned the entire risk spectrum. The risks arising in any given scenario would necessarily depend on context, making it impossible to place general-purpose AI into a single risk bucket.

Consequently, Europe's legislators ultimately proposed an entirely new chapter of the AI Act dedicated specifically to regulating general-purpose AI models: Chapter V.

Distinguishing AI models from AI systems

As identified in Part 1 of this series, the difference between AI models and AI systems is critical.

This is because Chapter V sets out rules that address the use of general-purpose AI models. While the AI Act also defines the concept of a general-purpose AI system as a system based on a general-purpose AI model. This term is simply a subset of the broader concept of an AI

system, and general-purpose AI systems are not addressed within Chapter V's rules.

Further, by specifying rules for general-purpose AI models, Chapter V takes a different regulatory approach from the one taken generally throughout the AI Act, which instead regulates AI systems, of which general-purpose AI systems are just one type. The rules applicable to an AI system, including any general-purpose AI systems, will be determined by whether they are prohibited, high or low risk.

This distinction is not accidental. According to Recital 97, "the notion of general-purpose AI models should be clearly defined and set apart from the notion of AI systems to enable legal certainty."

Article 3(63) of the act defines a general-purpose AI model as "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."

Therefore, to fully understand this definition, it is necessary first to understand what an AI model is and how it is different from an AI system.

The act does not define the concept of an AI model, but IBM helpfully explains "an AI model is a program that has been trained on a set of data to recognize certain patterns or make certain decisions without further human intervention." Recital 97 of the AI Act notes "AI models are essential components of AI systems" but "they do not constitute AI systems on their own." This is because "AI models require the addition of further components, such as for example a user interface, to become AI systems. AI models are typically integrated into and form part of AI systems."

An AI model can therefore be thought of as the program that powers the intelligence of an AI system, but it cannot be used on a stand-alone basis. Accordingly, an AI model must first be integrated with other software and/or hardware components, so users have a means to access and interact with the AI model via a user interface, such as using a dialogue box to submit prompts. The set of hardware and software components that integrate, and enable users to interact with, one or more AI models collectively comprise the AI system. For example, in very generalized terms, an autonomous vehicle can be thought of as an AI system that integrates multiple AI models to enable it to steer the vehicle, manage fuel consumption, apply brakes and so on.

What is a general-purpose AI model?

In general, the AI Act applies to AI systems, not AI models. As explained above, a general-purpose AI model:

- → Is an AI model, not an AI system, although it may be integrated into an AI system.
- → Is trained with a large amount of data using self-supervision at scale. For example, ChatGPT 3 was reportedly trained on at least 570 gigabytes of data or about 300 billion words.
- → Displays significant generality and is capable of competently performing a wide range of distinct tasks.

However, the act only regulates AI models that are placed on the EU market. "AI models that are used for research, development or prototyping activities before they are placed on the market" are excluded from the definition of a general purpose-AI model under Article 3(63) and from the scope of the act under Article 2(8).

Types of general-purpose AI models covered by the act

Chapter V distinguishes between general-purpose AI models with and without systemic risk. This distinction reflects the need to have stricter regulatory controls for general-purpose AI models with systemic risk due to their potential for significant harmful effects if not closely regulated.

To this end, under Article 3(65) of the AI Act, systemic risk is defined as "a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain."

At first glance, this definition appears circular. A general-purpose AI model with systemic risk is one presenting risks that would have significant impact and are "specific to the high-impact capabilities of general-purpose AI models." However, the definition hints at the types of concerns AI Act legislators believe general-purpose AI could present, namely "negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale."

As to what these "negative effects … propagated at scale" could include, Recital 110 lists "major accidents, disruptions of critical sectors and serious consequences to public health and safety; any actual or reasonably foreseeable negative effects on democratic processes, public and economic security; the dissemination of illegal, false, or discriminatory content."

It continues that these might result in "chemical, biological, radiological, and nuclear risks … offensive cyber capabilities … the capacity to control physical systems and interfere with critical infrastructure; risks from models of making copies of themselves or 'self-replicating' or training other models … harmful bias and discrimination … the facilitation of disinformation or harming privacy with threats to democratic values and human rights."

How to identify a general-purpose AI model with systemic risk

For the purposes of the AI Act, there are two ways for a general-purpose AI model to be deemed to present a systemic risk.

First, under Article 51(1-2), the general-purpose AI model must have "high impact capabilities," as evaluated by "appropriate technical tools and methodologies, including indicators and benchmarks."

For these purposes, a general-purpose AI model is presumed to have high impact capabilities if the cumulative amount of computation used for training is greater than 10^{25} floating point operations.

To put this in human terms, according to some estimates, the computational power of the human brain is approximately in the

order of 10^{16} to 10^{17} floating point operations. However, this is a crude and imprecise comparison for all sorts of reasons, not least that, while considerably slower than a computer, the brain is capable of much greater parallel processing at much lower levels of energy consumption. Nevertheless, it does provide a simple way for nonengineers to picture the type of computing power concerned.

Second, a general-purpose AI model can be determined to have high impact capabilities by the European Commission, which it can do either on its own initiative or following a qualified alert from the Scientific Panel of Independent Experts created under Articles 51(1)(b), 68 and 90 of the act. In reaching such a determination, the Commission must have regard to certain criteria set out in Annex XIII.

The Commission must publish a list of general-purpose AI models with systemic risk per Article 52(6) and can adopt delegated legislation to amend and supplement the thresholds, benchmarks and indicators that determine what qualify as high impact capabilities under Article 51(3) to keep pace with evolving technological developments.

Obligations for providers of all general-purpose AI models

Providers of general-purpose AI models with or without systemic risk must comply with the obligations set out in Article 53 and Article 54 of the AI Act. These primarily address technical documentation requirements, the provision of transparency information to providers of AI systems that integrate the general-purpose AI models, compliance with EU copyright rules and the need for non-EU model providers to appoint an EU representative.

Providers of general-purpose AI models without systemic risk have fewer obligations than those with systemic risk. For that reason, while providers of general-purpose AI models without systemic risk only need to comply with Articles 53 and 54, providers of models with systemic risk have additional compliance responsibilities under Article 55.

Obligations that apply to all providers of general-purpose AI models, with or without systemic risk, include the following:

- Prepare and maintain technical documentation about the general-purpose AI model, including its training and testing process and evaluation results, containing the mandatory information set out in Annex XI, listed in the Annex section below. The European Commission's AI Office and national competent authorities can require the general-purpose AI model provider to provide this documentation on request. See also Article 91(1).

- Make certain information and documentation available to providers of AI systems that integrate the general-purpose AI model so they have a good understanding of the capabilities and limitations of the model and can comply with their own obligations under the AI Act. This must include the mandatory information set out in Annex XII, listed in Table 2.

- Put a policy in place to comply with EU copyright and related rights rules. This should include a means to identify and comply, through state-of-the-art technologies, with any reservation of rights expressed by rights holders.

→ Prepare and make publicly available a detailed summary of the general-purpose AI model's training content using a template provided by the AI Office that is not yet available as of the date of this article. This latter requirement has raised eyebrows among providers of general-purpose AI models over concerns that it may force them to reveal trade secrets about their training content.

The first two points above do not apply to providers of open-source general-purpose AI models unless they have systemic risk, provided these models can be used and adapted without restriction and that information about their parameters, including weights, model architecture and model usage are made publicly available.

In addition, and with more than a passing nod toward EU representative requirements under the EU General Data Protection Regulation, non-EU providers of general-purpose AI models must additionally appoint an authorized representative in the EU per Article 54(1). This appointment must be via a written mandate that authorizes the representative to:

→ Verify that the general-purpose AI model provider has prepared the required technical documentation and otherwise fulfilled its obligations under Article 53, as described above, and Article 55, if it provides a general-purpose AI model with systemic risk, as described below.

→ Keep a copy of the general-purpose AI model provider's required technical documentation for a period of 10 years after the model is placed on the market, so it is available to the European Commission's AI Office and national competent authorities, in addition to its contact details.

→ Provide the AI Office with the compliance information and documentation necessary to demonstrate the general-purpose AI model provider's compliance upon request.

→ Cooperate with the AI Office and competent authorities upon request in any action they take in relation to the general-purpose AI model, including when it is integrated into AI systems available in the EU.

Once again, this requirement does not ordinarily apply to providers of open-source general-purpose models, unless those models have systemic risk.

Obligations of providers of general-purpose AI models with systemic risks

As already noted, providers of general-purpose AI models with systemic risk are subject to additional obligations under Article 55 of the AI Act. In addition to the rules already described above, they must also:

→ Perform model evaluation in accordance with standardized protocols and tools reflecting the state of the art, including conducting and documenting adversarial testing of the model with a view to identifying and mitigating the systemic risks described above.

→ Assess and mitigate possible systemic risks at an EU level, including their sources, that may stem from the development, sale or use of general-purpose AI models with systemic risk.

- → Keep track of, document and report relevant information about serious incidents without undue delay to the AI Office, and to national competent authorities as appropriate, including possible corrective measures.

- → Ensure an adequate level of cybersecurity protection for the general-purpose AI model with systemic risk and the physical infrastructure of the model.

Regarding the requirement to document and report relevant information about serious incidents, a key question is how this requirement will be operationalized in practice, and further guidance would be welcomed in this respect. However, it is clear that this requirement is distinct from the requirement for high-risk AI systems' providers and deployers to report serious incidents under Article 26(5) and Article 73.

Codes of practice for general-purpose AI

To demonstrate their compliance and pending the EU's adoption of harmonized standards for general-purpose AI, pursuant to Article 40, providers of general-purpose AI models, with or without systemic risk, can adhere to codes of practice which are expected to be drawn up and finalized by the AI Office within nine months after the AI Act enters into force. This would follow consultation with the AI Board and national competent authorities, as well as industry, academic and civil society stakeholders under Article 56.

The European AI Office launched a consultation for a first Code of Practice for general-purpose AI models 30 July 2024.

When does this take effect?

The AI Act's rules for general-purpose AI model providers come into effect in two phases under Articles 111(3) and 113.

Providers of older general-purpose AI models placed on the EU market before 2 Aug. 2025 have up to three years from the act's entry into force to comply, i.e. until 2 Aug. 2027. However, providers of newer general-purpose models, that is, all other general-purpose AI model providers, have up to 12 months after the act enters into force to come into compliance, i.e. until 2 Aug. 2025.

Practical steps for general-purpose AI

Any organization using general-purpose AI will need to ask itself the following questions and implement compliance measures accordingly:

- → Is the general-purpose AI in question a general-purpose AI model to which Chapter V applies or, instead, a general-purpose AI system that must then be categorized as prohibited, high or low risk to determine which rules apply under the AI Act?

- → Is the organization in question the provider of the general-purpose AI model? Chapter V applies only to providers of general-purpose AI models.

- → Does the general-purpose AI model present systemic risk? If not, it will be subject only to the rules in Articles 53 and 54. If so, it will be subject to additional rules in Article 55.

- → Has the AI Office produced any applicable codes of practice yet under Article 56?

If so, consider alignment with these as a means of demonstrating compliance with the AI Act.

→ Is the general-purpose AI model provider established outside the EU? If so, it must appoint an authorized representative in the EU in accordance with Article 54.

→ Are you a provider of an older or newer general-purpose AI model for the purposes of Articles 111(3) and 113? This will determine when the AI Act's rules apply to you, and when you need to come into compliance.

Annex

Mandatory information to be included in technical documentation for general-purpose AI models

WITH OR WITHOUT SYSTEMIC RISK	WITH SYSTEMIC RISK
A general description of the general-purpose AI model, including: → The tasks that the model is intended to perform and the type and nature of AI systems in which it can be integrated. → The acceptable use policies applicable. → The date of release and methods of distribution. → The architecture and number of parameters. → The modality, such as text or image, and format of inputs and outputs. → The license. A detailed description of the elements of the model referred to above and relevant information of the process for the development, including the following elements: → The technical means required to integrate the general-purpose AI model in AI systems, such as instructions for use, infrastructure and tools. → The design specifications of the model and training process, including training methodologies and techniques. The key design choices include the rationale and assumptions, what the model is designed to optimize, and the relevance of the different parameters. → Information on the data used for training, testing and validation, when applicable, including the type and provenance of data and curation methodologies, such as cleaning and filtering; the number of data points, their scope and main characteristics; how the data was obtained and selected; as well as all other measures to detect the unsuitability of data sources and methods to detect identifiable biases, when applicable. → The computational resources used to train the model, such as the number of floating point operations, training time and other relevant details related to the training → The known or estimated energy consumption of the model. When the energy consumption of the model is unknown, the energy consumption may be based on information about computational resources used.	→ A detailed description of the evaluation strategies, including evaluation results, based on available public evaluation protocols and tools or other evaluation methodologies. Evaluation strategies shall include evaluation criteria, metrics and methods for identifying limitations. → A detailed description, when applicable, of the measures implemented to conduct internal and/or external adversarial testing, such as red teaming and model adaptations, including alignment and fine tuning. → When applicable, a detailed system architecture description that explains how software components build or feed into each other and integrate into the overall processing.

Mandatory transparency information for general-purpose AI models

WITH OR WITHOUT SYSTEMIC RISK

A general description of the general-purpose AI model including:

- → The tasks that the model is intended to perform and the type and nature of AI systems into which it can be integrated.
- → The acceptable-use policies applicable.
- → The date of release and methods of distribution.
- → How the model interacts, or can be used to interact, with hardware or software that is not part of the model itself, when applicable.
- → The versions of relevant software related to the use of the general-purpose AI model, when applicable.
- → The architecture and number of parameters.
- → The modality, such as text or image, and format of inputs and outputs.
- → The license for the model.

A description of the elements of the model and of the process for its development, including:

- → The technical means required to integrate the general-purpose AI model into AI systems, such as instructions for use, infrastructure and tools.
- → The modality, like text or image, and format of the inputs and outputs and their maximum size, such as context or window length.
- → Information on the data used for training, testing and validation, when applicable, including the type and provenance of data and curation methodologies.

Published September 2024

Governance: EU and national stakeholders

By Laura Pliauskaite and Isabelle Roccia

The EU AI Act sets up an intricate governance structure with various stakeholders at both the EU and national levels to ensure its effective and coherent implementation and enforcement. Chapter VII of the AI Act provides an overview of this structure but certain details concerning specific roles, tasks and interactions can be found beyond this section. Also, Chapter VII does not mention all the actors involved in the act's implementation and enforcement.

This article focuses on each body, outlining its composition and main competences to help organizations better understand the AI Act's governance structure. While indicating every task of each stakeholder is beyond the scope of this article, the annex below navigates the AI Act's text to find their responsibilities.

Who is responsible for the AI Act's governance at the EU level?

Besides initiating the AI Act, the European Commission is also an important facilitator of its implementation and enforcement. Along with other bodies, many of which are newly established at the EU level, it aims to ensure consistent application of the AI Act across the EU.

AI Office

The AI Act does not provide much information on the composition of the AI Office. Its current set up, effective as of 16 June, only became clear months after the publication of the European Commission decision that officially established it in January 2024. The AI Office was not built completely from scratch. The Commission renamed and reorganized an existing unit, the Directorate-General for Communications Networks, Content and Technology Directorate A for Artificial Intelligence and Digital Industry, with five topic-specific units and two sections with an advisory function. The AI Office is led by Lucilla Sioli, former Directorate A director.

In its initial stages, the AI Act envisioned the European Commission and the AI Office as having two distinct roles. The notion of the AI Office has evolved since then. As previously stated, it is currently set up as part of the Commission's administrative structure and is therefore a component of the Commission. According to the final AI Act text, the AI Office

is "the Commission's function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance, provided for in Commission Decision of 24 January 2024."

However, the AI Act identifies and refers to both the Commission and the AI Office throughout its text. The confusion stemming from the text must be recognized. It is no more than a consequence of expeditious negotiations and pressure to publish the AI Act before summer recess, resulting in a lack of time to properly clean up its final wording. To avoid further confusion, this article will refer to the Commission's and the AI Office's competences under the AI Act as the AI Office.

The AI Office plays an important role in realizing the AI Act's goals and is therefore assigned a multitude of responsibilities for facilitating its implementation, including:

- → Issuing standardization requests to European standardization organizations that must translate the AI Act's rules and obligations into specific technical requirements.
- → Adopting secondary legislation, such as delegated and implementing acts, to clarify the AI Act's rules and obligations and to ensure it stays relevant. They will cover topics including criteria and use cases for high-risk AI and common specifications for areas without suitable harmonized standards.
- → Issuing guidelines on practical implementation of the AI Act, including on the application of requirements and obligations for high-risk AI systems.
- → Setting up and maintaining various databases, including on general-purpose AI models with systemic risks, high-risk AI systems listed in Annex III, information on notified bodies and AI regulatory sandboxes.
- → Ensuring effective support mechanisms for national competent authorities, for instance by facilitating the creation and operation of AI regulatory sandboxes and coordinating joint investigations of national market surveillance authorities.
- → Supporting relevant sectoral bodies with implementing rules on prohibited AI practices and high-risk AI systems.
- → Facilitating the drawing up of codes of conduct and codes of practice at the EU level and monitoring the implementation and evaluation of the latter.
- → Facilitating compliance with the AI Act, particularly of small- and medium-sized enterprises, including by providing standardized templates upon the AI Board's request and raising awareness about the AI Act's obligations.
- → Ensuring the rules of the AI Act and other EU legislation in the digital field where the Commission holds supervisory and enforcement powers, such as the Digital Markets Act and Digital Services Act, are applied to AI systems in a coordinated manner.
- → Assisting other bodies at the EU level with organizational matters. The AI Office acts as the secretariat for the AI Board and

provides administrative support for the Advisory Forum and the Scientific Panel of Independent Experts.

The AI Office is also tasked with the supervision, monitoring and enforcement of rules concerning general-purpose AI models and is supported in these tasks by the Scientific Panel. Specifically, the AI Office is tasked with:

- Developing resources for evaluating general-purpose AI capabilities and monitoring the emergence of unforeseen general-purpose AI risks.
- Conducting investigations and requesting information from the operators of general-purpose AI models.
- Adopting mitigation measures, corrective measures and sanctions in case of infringements.
- Acting as a market surveillance authority for AI systems based on general-purpose AI models when the model and system are provided by the same provider.

The AI Office periodically reviews certain aspects of the AI Act and will evaluate it as a whole five years after it enters into force and every four years after. It also evaluates various decisions adopted at a national level, including:

- Measures adopted by national market surveillance authorities against operators of AI systems. When there is a dispute between member states concerning their suitability, it has the decisive authority to determine whether these measures must be followed in other member states or whether they are inadequate and must be withdrawn.
- Instances in which market surveillance authorities authorize the deployment of high-risk AI systems without prior conformity assessments.
- The competence of notified bodies. It may investigate their competence when in doubt and even adopt corrective measures.

The Commission decision establishing the AI Office states it will work in close cooperation with various stakeholders at sectoral, national and EU levels when carrying out its tasks. However, their relationship with the AI Office and other EU bodies is not clear cut. For instance, in a situation that concerns financial services and AI, questions about how the competencies of the AI Office and the European Central Bank will intersect arise.

It should be noted the competences of the AI Office are not restricted to the AI Act. The AI Office has a central role in the EU concerning the development, launch and use of trustworthy AI. It is also tasked with promoting the EU approach to trustworthy AI on the international stage.

AI Board

The AI Board was established to ensure consistent and effective application of the AI Act across the EU. It provides a platform for dialogue and coordination between national competent authorities for sharing expertise and best practices, identifying common issues and ways to collectively address them, and working to harmonize administrative practices, for

instance concerning derogation from conformity assessment procedures and the functioning of AI regulatory sandboxes.

The AI Board advises the AI Office and member states on the AI Act's implementation. It issues recommendations and opinions on various matters, including on:

- → Qualified alerts regarding general-purpose AI models.
- → The development and application of codes of conduct and codes of practice.
- → The use of harmonized standards.
- → The need to revise certain sections of the AI Act.
- → AI trends and international matters on AI.

The AI Board is composed of one representative per EU member state who serves a three-year mandate, the European Data Protection Supervisor as an observer and the AI Office without voting rights. Depending on the meeting's agendas, an invitation may be extended to other national and EU bodies. The AI Board consists of two standing subgroups, though additional standing or temporary subgroups may be established if needed.

AI Advisory Forum

Upon request, the AI Advisory Forum provides the AI Board and the AI Office with technical expertise, recommendations, opinions and other written contributions on matters including harmonized standards and commons specifications. It may also set up standing or temporary subgroups to analyze specific AI Act-related issues. Anyone interested in the yearly activities of the AI Advisory Forum will be able to consult its publicly accessible reports.

The AI Advisory Forum is comprised of members appointed by the AI Office with AI expertise representing a balanced selection of stakeholders from industry, including startups and SMEs, civil society and academia. The EU Fundamental Rights Agency, the EU Agency for Cybersecurity and the European standardization organizations are its permanent members. This balanced representation ensures both commercial and noncommercial interests are considered when contributions from the AI Advisory Forum are requested. Some suggest the European AI Alliance, a European Commission initiative with the goal of creating an open policy dialogue on AI, will take up the role of the AI Advisory Forum, but that is not yet confirmed.

Scientific Panel of Independent Experts

The main role of the Scientific Panel of Independent Experts is to support the AI Office in monitoring general-purpose AI models. Its tasks include:

- → Alerting the AI Office of general-purpose AI models with systemic risks at the EU level.
- → Contributing to the development of resources for evaluating general-purpose AI capabilities and other tools and templates.
- → Advising the AI Office on the classification of general-purpose AI models.
- → Supporting market surveillance authorities and their cross-border activities.

Providing EU member states with access to their pool of experts, possibly for a fee.

The panel consists of experts selected by the AI Office who are knowledgeable in a range of topics in the field of AI. They must be able to demonstrate such scientific or technical expertise. Additionally, they must be independent from any provider of AI systems or general-purpose AI models, perform their tasks fully independently and objectively, and respect confidentiality requirements. The composition of the panel must be balanced geographically and gender-wise to ensure a fair EU-wide representation.

EDPS

The EDPS' principal role is to ensure the EU bodies' compliance with European data protection rules. The AI Act assigns it additional competences by designating it as a market surveillance authority for the EU bodies concerning their implementation of the AI Act. In this role, it may establish an AI regulatory sandbox to provide the EU bodies with a safe testing environment. In case of their noncompliance, the EDPS may impose administrative fines.

EU AI testing support structures

The EU AI testing support structures are bodies, either at national or EU level, that are designated by the AI Office to support market surveillance actions on AI in the EU. They increase the capacity of national market surveillance authorities by testing products upon their or the AI Office's request and by developing new techniques and methods of analysis. They must also provide independent technical or scientific advice when requested by the AI Office, market surveillance authorities or the AI Board.

European standardization organizations

European standardization organizations, such as the European Telecommunications Standards Institute, the European Committee for Standardization and the European Committee for Electrotechnical Standardization, play an important role in supporting the implementation of EU legislation and policies, as they develop standards that facilitate compliance with their rules and obligations.

When it comes to the AI Act, the latter two bodies have established the Joint Technical Committee 21 on AI. The committee is divided into topic-specific working groups of experts, which, upon receiving a standardization request from the AI Office, work on developing harmonized standards that translate the rules and obligations of the AI Act into concrete technical requirements. Once such a standard is developed and awarded a harmonized standard status, it may then be voluntarily adopted to showcase compliance with a specific requirement of the AI Act.

Who is responsible for the AI Act's governance at the national level?

Member states are responsible for implementing and enforcing the AI Act on a national level. They are supported in this role by national competent authorities and other bodies established at a national level.

Member states

Member states must designate national competent authorities 12 months after the AI Act enters into force and ensure they have sufficient resources, sufficient competences and a proper infrastructure.

Member states are also responsible for establishing rules on the AI Act's enforcement

measures, such as penalties and administrative fines but also warnings and other nonmonetary measures. The rules must be in accordance with the requirements set out in the AI Act itself, as well as the AI Office's guidelines on this matter.

Member states also have the power, with certain limits, to put laws in place to authorize the use of real-time biometric identification systems fully or partially in publicly accessible spaces for the purpose of law enforcement. They may also introduce more restrictive laws on the use of real-time remote and post-remote biometric identification systems.

National competent authorities

Member states must designate at least one market surveillance authority and one notifying authority, as well as choose one market surveillance authority as a single point of contact for matters concerning the AI Act. Depending on their specific needs, member states may designate more than one of each type of authority.

At this moment, several approaches are emerging. Denmark appointed its Agency for Digital Government, Italy's national data protection authority expressed its interest in taking up the role and Spain chose to create a new authority called the Agencia Española de Supervisión de la Inteligencia Artificial from scratch. Regardless of the approach, significant capacity building will be needed to equip authorities for their new responsibilities, whether in terms of staffing, budget or expertise. For instance, DPAs will need to acquire competencies not in their typical lines of work, akin to product-safety supervision and enforcement.

While national competent authorities oversee the implementation of the AI Act, they also facilitate it. They must establish new or participate in existing AI regulatory sandboxes individually or jointly with other member states' competent authorities, supervise their use and report on it to the AI Office and the AI Board. SMEs have to be given priority access to such AI regulatory sandboxes. In their facilitatory role, national competent authorities must also provide guidance, especially to SMEs, on the AI Act's implementation and assist with drawing up codes of conduct. They must ensure their independence and impartiality in carrying out their tasks.

Market surveillance authorities

Market surveillance authorities monitor and investigate AI systems' compliance with the AI Act, including classifying AI systems as nonhigh risk. They can request any information that may be relevant to their investigations from providers and deployers. They can carry out such investigations and other activities jointly with other member-state market surveillance authorities, particularly when it comes to high-risk AI systems that present serious risks in cross-border cases or in cooperation with the AI Office in certain cases concerning general-purpose AI or high-risk AI. They must also cooperate and coordinate their activities with sectoral market surveillance authorities when relevant. However, the relationship between different authorities is somewhat unclear, which may create issues in situations where competences overlap.

In the event of noncompliance, market surveillance authorities adopt measures, including corrective action and restricting or prohibiting AI systems from the EU market. In the latter case, the authority informs the AI Office and other member-state authorities of such noncompliance and the measures taken. The same goes for when noncompliance is not

restricted to the national territory of the market surveillance authority concerned. If the AI Office or other national authorities object to such measures, the lead market surveillance authority must consult the AI Office and the operators concerned. If the AI Office then deems the measures appropriate, they must be adopted by other member-state authorities and if not, they must be withdrawn.

If a high-risk AI system is found to be compliant but presents a risk to the health or safety of people, to fundamental rights, or to other aspects of public interest protection, the market surveillance authority should request it to eliminate that risk through appropriate measures. The market surveillance authority must inform the AI Office and other member states of the high-risk AI system in question, the risk it presents and the measures taken. It must enter into consultation with the AI Office and the member states and operators concerned. The AI Office may then request the adoption of different measures as necessary.

Market surveillance authorities must not only track compliance but also handle complaints they receive from companies and individuals. The procedures for doing so are left to authorities themselves. Additionally, they must collect serious incident reports from high-risk AI system providers and, in certain cases, notify such incidents to authorities protecting fundamental rights.

Apart from overseeing AI systems compliance with the AI Act, market surveillance authorities may authorize deploying high-risk AI systems without prior conformity assessments for exceptional reasons, such as public security, and for a limited period while completing the required conformity assessment procedures. In such cases, they must inform the AI Office and other member states and, if objections are raised, enter consultations with the AI Office. The AI Office may request the market surveillance authority withdraw the authorization if it is deemed unjustified.

Additionally, market surveillance authorities supervise the testing of AI systems in real-world conditions, handle applications for testing high-risk AI systems in real-world conditions outside AI regulatory sandboxes and monitor the testing when needed.

Finally, market surveillance authorities are required to share any relevant findings from their activities with the AI Office and other relevant stakeholders, such as competition authorities, and report to the AI Office on the use of real-time biometric identification systems.

With such pivotal responsibilities under the AI Act, it is fair to say market surveillance authorities are the central point of interest for AI system operators in the EU.

Notifying authorities

Notifying authorities assess, designate, notify and monitor conformity assessment bodies. They develop procedures for such activities collectively with other member-state notifying authorities and must generally coordinate their activities and cooperate, including by exchanging best practices. They must also ensure bodies notified by them participate in the sectoral group of notified bodies to enhance coordination and cooperation.

In case of doubt, notifying authorities investigate notified bodies' competences

and take necessary measures, including suspending or withdrawing notifications. They must communicate all notifications and any changes to the AI Office and other member states.

There should be no conflict of interest between notifying authorities and conformity assessment bodies. Notifying authorities must respect confidentiality obligations and perform their duties objectively and impartially, for instance by having different people carry out assessing and notifying activities.

Notified bodies

Notified bodies are conformity assessment bodies accredited to perform conformity assessment activities, such as testing, inspecting and certifying high-risk AI systems. They also determine the procedures for carrying out such activities. They must cooperate and coordinate with other notified bodies in the form of a sectoral group of notified bodies.

Notified bodies may perform conformity assessment procedures fully or partially through subcontractors or subsidiaries that comply with the same requirements applicable to them. In such cases, notified bodies must make the information public and inform notifying authorities.

To be accredited as a notified body, an organization must fulfil certain requirements. For instance, it must:

- → Be established in an EU member state. In certain cases, third-country establishments may be authorized to perform notified bodies' activities.
- → Be independent from providers of AI systems under conformity assessments and their competitors.
- → Not be directly involved in designing, developing, marketing or using high-risk AI systems, or represent parties that are.
- → Ensure expertise, impartiality, objectivity, confidentiality and independence of its activities, safeguarded by documented procedures.
- → Provide all relevant documentation confirming its activities and competences to the notifying authority of the country of its establishment.
- → Be informed about current relevant standards, for instance through direct or representative participation in European standardization organizations.

National authorities protecting fundamental rights

As the protection of fundamental rights is crucial under the AI Act, national public authorities protecting them also play a role in the act's enforcement. When such an authority suspects the use of a high-risk AI system identified in Annex III may breach EU fundamental rights obligations, it can request and access any documentation created or maintained under the AI Act to determine the existence of such a breach, while ensuring confidentiality obligations are respected. If a request is made, the authority protecting fundamental rights must inform the relevant market surveillance authority. It may request the market surveillance authority to perform

technical testing of the AI system in question if the documentation obtained is not sufficient to identify a breach.

Member states must publish and maintain a public list of national public authorities that protect fundamental rights.

DPAs

While EU member states are free to designate DPAs as their national competent authorities responsible for implementing and enforcing the AI Act, they are already assigned the task of a market surveillance authority concerning certain high-risk AI systems, including those listed in points 6, 7 and 8 of Annex III. In addition, DPAs are involved in the operation and supervision of AI regulatory sandboxes when they are used by AI systems that process personal data.

They must also gather information on the use of real-time and post-remote biometric identification systems and report annually on the use of the former to the AI Office.

Law enforcement or civil protection authorities

Law enforcement or civil protection authorities are given the power to use real-time remote biometric identification systems in publicly accessible spaces in specific and limited situations only when permitted by member-state law. In addition, certain requirements must be fulfilled:

- → A fundamental rights impact assessment must be completed before such use.
- → The use must be preauthorized by a judicial or independent administrative authority, unless it concerns a situation of urgency.
- → Real-time remote biometric identification systems must be registered in the EU database.
- → Each use of such a system must be notified to the relevant market surveillance authorities and DPAs.

The AI Office reviews such authorizations and may deem them unjustified. In such cases, their use must be stopped and resulting outputs must be discarded immediately.

Furthermore, the AI Act allows law enforcement or civil protection authorities to deploy specific high-risk AI systems without preauthorization by a market surveillance authority. However, this is only allowed for exceptional reasons, including threats to public security or the safety of individuals. Even if such conditions are met, the authority in question must request the authorization without undue delay and, if it is rejected, immediately stop the use of the system and discard resulting outputs.

Judicial authorities or independent administrative bodies

Judicial authorities or independent administrative bodies can authorize the deployment of real-time remote biometric identification systems in publicly accessible spaces for law enforcement in specific and limited situations only when permitted by law in the member state concerned.

Annex

This section outlines the different EU and national stakeholders, and the articles and recitals of the EU AI Act in which their competences and compositions are referenced.

AI Advisory Forum	SUPPORT, ADVICE	COMPOSITION
	Described in the below articles and recitals of the EU AI Act. → Articles: 40(2), 41(1), 65(6), 67 → Recitals: 121, 148	Described in the below articles and recitals of the EU AI Act. → Articles: 67 → Recitals: 150
AI Board	SUPPORT, ADVICE	COMPOSITION
	Described in the below articles and recitals of the EU AI Act. → Articles: 6(5), 40(2), 56(2,4,6), 57(8,14-16), 62(3a), 66, 68(2), 70(6,8), 71(1), 75(2), 84(2), 90(2), 92(1), 101(4), 112(8,9) → Recitals: 20, 53, 121, 143, 150, 161	Described in the below articles and recitals of the EU AI Act. → Articles: 65 → Recitals: 148, 149
DPAs	ENFORCEMENT	EX-POST EVALUATION
	Described in the below articles and recitals of the EU AI Act. → Articles: 5(4), 26(10), 57(10), 74(8) → Recitals: 36, 157, 159	Described in the below articles and recitals of the EU AI Act. → Articles: 5(6) → Recitals: 36
EDPS	ENFORCEMENT	EX-POST EVALUATION
	Described in the below articles and recitals of the EU AI Act. → Articles: 3(48), 57(3), 58(2g), 65(2), 70(9), 74(9) → Recitals: 156, 168	Described in the below articles and recitals of the EU AI Act. → Articles: 100
EU AI testing support structures	SUPPORT, ADVICE	
	Described in the below articles and recitals of the EU AI Act. → Articles: 84 → Recitals: 145, 152	

<table>
<tr><td rowspan="8">European Commission through the AI Office</td><td>IMPLEMENTATION</td><td>ENFORCEMENT</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(5,6), 11(1), 15(2), 25(4), 27(5), 30(2), 35, 38, 50(7), 52(6), 53(1d), 56, 57(1,15,17), 62(3), 67(3), 68(2,4), 69(3), 70(2), 71(1), 84(1), 95, 112(11)
→ Recitals: 20, 49, 74, 90, 96, 107, 111, 116, 117, 126, 127, 131, 135, 141, 145, 147, 149, 152, 160, 165, 179</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 30(4,5), 36, 37, 46(3-5), 49(4), 52, 53(1,4), 54(3-5), 55(1c,2), 56, 57(8,11,16), 62(3d), 64, 65(2,8), 66(e), 67(8), 70(6,7), 71(6), 73(11), 74(2,11), 75(1-3), 77(2), 78, 79(3,5,7,8), 80(3), 81, 82, 84(2), 88(1), 89, 90, 91(1-4), 92, 93, 96(2), 99(2,11), 100(7), 101-110
→ Recitals: 20, 36, 37, 78, 101, 108, 111-113, 115, 117, 124, 126, 131, 143, 149-151, 160-164, 166, 169, 179</td></tr>
<tr><td>EX-POST EVALUATION</td><td>SECONDARY LEGISLATION</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(7), 97(2), 112
→ Recitals: 174</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 6(6,7), 7, 11(3), 37(4), 41(1,2,4,6), 43 (5,6), 47(5), 50(7), 51(3), 52(4), 53(3,5,6), 56(6,9), 58(1,2), 60(1), 68(1,5), 72(3), 92(6), 97, 98(2), 101(6)
→ Recitals: 52, 101, 117, 121, 173, 175</td></tr>
<tr><td>GUIDELINES</td><td>STANDARDS AND COMMON SPECIFICATIONS</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 6(5), 63(1), 73(7), 96
→ Recitals: 53, 81, 146</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 40(2), 41
→ Recitals: 81, 121</td></tr>
<tr><td colspan="2">COMPOSITION</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 3(47)
→ Recitals: 148</td></tr>
<tr><td rowspan="2">European standardization organizations</td><td colspan="2">IMPLEMENTATION</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 40, 41(1a,4), 58(2f), 67(5)
→ Recitals: 27, 121, 139</td></tr>
<tr><td rowspan="2">Judicial authorities or independent administrative bodies</td><td colspan="2">ENFORCEMENT</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(3), 26(10)
→ Recitals: 22, 35, 61</td></tr>
</table>

<table>
<tr><td rowspan="2">Law enforcement or civil protection authorities</td><td colspan="2">ENFORCEMENT</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(2-4), 26(10), 43(1), 46(2), 59(2), 72(2), 78(3)
→ Recitals: 33, 34, 35, 38, 59, 130, 155</td></tr>
<tr><td rowspan="4">Market surveillance authorities</td><td>ENFORCEMENT</td><td>EX-POST EVALUATION</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(4), 20(2), 22(3,4), 26(5,10), 27(3), 36(6), 43(1), 46, 57(7), 60(4,6-8), 66(a), 68(3b,c), 70(1,2), 71(4), 73(1,7,8), 75(1-3), 76, 77(1,3), 78-83, 84(2), 85, 88(2)
→ Recitals: 36, 96, 130, 131, 141, 149, 156, 158, 159, 160, 161, 162, 170</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 5(6), 74(2)
→ Recitals: 36</td></tr>
<tr><td colspan="2">COMPOSITION</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 3(26), 74
→ Recitals: 153</td></tr>
<tr><td rowspan="4">Member states</td><td>IMPLEMENATION</td><td>ENFORCEMENT</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 2(11), 4, 5(5), 18(2), 26(10), 28(1,2), 57(1-4), 60(6), 62(1), 65(2-4), 66(o), 70, 71(1), 77(2), 95, 96(2), 99, 113
→ Recitals: 1, 3, 9, 20, 22, 24, 33, 37, 60, 72, 80, 94, 129, 138, 142, 143, 145, 148, 149, 153, 158, 168, 179</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 2(3,4), 30(2-5), 31(9), 36(1,4,7b,7d,9), 37(4), 41(6), 46(3-5), 58(2g), 64(2), 69(1,2), 70, 74(3,7,8,10), 78(4,5), 79(3,5,7), 80(3), 81, 82, 88(1), 97(4), 113
→ Recitals: 126, 131, 151, 152, 153</td></tr>
<tr><td colspan="2">EX-POST EVALUATION</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 99(11), 112(8)
→ Recitals: 179</td></tr>
<tr><td rowspan="2">National authorities protecting fundamental rights</td><td colspan="2">ENFORCEMENT</td></tr>
<tr><td colspan="2">Described in the below articles and recitals of the EU AI Act.
→ Articles: 77, 79(2)
→ Recitals: 139</td></tr>
</table>

<table>
<tr><td rowspan="2">National competent authorities</td><td>ENFORCEMENT</td><td>COMPOSITION</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 6(4), 16(k), 17(1j), 18(1), 21, 23(6,7), 24(4-6), 26(12), 36(7e,8b,9), 47(1), 49(4), 53(1a,3), 54(3,4), 55(1c), 56(3), 57, 58(2,4), 59(1j), 65(6), 66(g,j,k), 70, 73(6, 10,11), 77(4), 78, 79(2), 99(7), Articles 112(4a, 8)
→ Recitals: 53, 68, 85, 101, 115, 116, 138-141, 149, 154, 157, 158, 167</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 3(48), 70
→ Recitals: 153</td></tr>
<tr><td rowspan="3">Notified bodies</td><td>IMPLEMENTATION</td><td>ENFORCEMENT</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 31, 32, 35
→ Recitals: 123-125, 143</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 11(1), 17(1j), 18(1c,d), 20(2), 22(4), 29-39, 43(1-3,6), 44, 45, 48(4), 57(7), 58(2f), 65(6), 73(6), 79(2), 99(4-5)
→ Recitals: 68, 127, 139, 145, 149</td></tr>
<tr><td colspan="2">COMPOSITION

Described in the below articles and recitals of the EU AI Act.
→ Articles: 3(22), 31, 39
→ Recitals: 126, 127, 179</td></tr>
<tr><td rowspan="3">Notifying authorities</td><td>IMPLEMENTATION</td><td>ENFORCEMENT</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 28</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 28-30, 33, 34(3), 36, 37(2), 38(2), 45(1), 70(1), 78
→ Recitals: 126, 149</td></tr>
<tr><td colspan="2">COMPOSITION

Described in the below articles and recitals of the EU AI Act.
→ Articles: 3(19), 28
→ Recitals: 153</td></tr>
<tr><td rowspan="3">Scientific Panel of Independent Experts</td><td>ENFORCEMENT</td><td>SUPPORT, ADVICE</td></tr>
<tr><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 51(1b), 52(4)
→ Recitals: 164</td><td>Described in the below articles and recitals of the EU AI Act.
→ Articles: 68, 69, 90, 91(3), 92(1b,2)
→ Recitals: 116</td></tr>
<tr><td colspan="2">COMPOSITION

Described in the below articles and recitals of the EU AI Act.
→ Articles: 68
→ Recitals: 151</td></tr>
</table>

Published September 2024

AI assurance across the risk categories

By Ashley Casovan and Osman Güçlütürk

Previous articles in this series have reflected on the scope and oversight requirements of the EU AI Act. Given the vast uses of AI, as well as the significant potential harm these systems carry, the assurance requirements embedded into the act provide important checks and balances.

While AI assurance is not defined in the AI Act, it is increasingly used in the AI ecosystem and is inspired by assurance mechanisms in other industries, such as accounting and product safety. The U.K. government defines assurance as "the process of measuring, evaluating and communicating something about a system or process, documentation, a product or an organisation. In the case of AI, assurance measures, evaluates and communicates the trustworthiness of AI systems." Similar mechanisms in the AI Act include a spectrum of oversight functions, including standards, conformity assessments and audits.

In relation to the AI Act, AI assurance mechanisms establish comprehensive processes and activities to measure and ensure a given AI system or general-purpose AI model adheres to specific obligations and requirements. Assurance is distinct from compliance. While compliance involves meeting set standards and regulations, assurance encompasses a broader and deeper evaluation to build confidence in an AI system's reliability and safety.

Broad vs. narrow perspectives of assurance

Assurance can be understood in broad and narrow senses.

Broad perspective

From a broader standpoint, assurance covers all actions taken to ensure and measure the compliance of an AI system with relevant rules, in this case, the AI Act. This includes ongoing monitoring, internal audits and assessments to provide a holistic view of the system's adherence to regulations.

Narrow perspective

In a narrower sense, assurance can be distinguished from official conformity assessment procedures. It refers specifically

to private or internal evaluations that do not carry the formal recognition of official assessments but still contribute to the overall trustworthiness and reliability of the AI system.

These perspectives are often used interchangeably. It is important to keep this mind when discussing AI assurance mechanisms.

Utilizing AI assurance tools can undoubtedly aid in measuring and mitigating risks, thereby facilitating preparation for compliance with the AI Act and the conformity assessments thereof. However, certifications from private AI assurance tools or companies do not indicate that an AI system or model officially meets the AI Act's requirements and do not carry the legal weight of an official conformity assessment. To fully grasp the role and implications of AI assurance under the AI Act, it is essential to examine the interaction between AI assurance and AI Act compliance.

Interaction of AI assurance with AI Act compliance

The EU AI Act, as a pioneering legislative framework, introduces a risk-based regulatory approach to AI governance. It provides a set of different requirements and obligations for AI systems and general-purpose AI models depending on their risk classifications. The obligations also vary for each type of operator, with the provider having the most stringent obligations.

The AI Act does not have a general one-stop compliance route or compliance assessment procedure. As the most strictly regulated subject under the act, high-risk AI systems have a specific procedure to assess whether a given high-risk AI system meets the requirements for these systems — the conformity assessment procedure. All high-risk AI systems must undergo a conformity assessment before entering the market. Conformity assessments ensure high-risk systems meet the stringent requirements before being marketed in the EU. On the other hand, the conformity assessment procedure is formalistic in terms of scope. It is provided only for AI systems and not for general-purpose AI models. It covers only the requirements provided under Chapter III Section 2 of the AI Act and not all obligations, which vary for different types of actors.

Depending on factors such as the system's intended purpose and the use of official EU standards, the assessment may be internal or require third-party involvement. There are two main conformity assessment procedures under the act.

Under the internal self-assessment, outlined in Annex VI, providers can conduct internal control procedures, which involve verifying that their quality management system and technical documentation comply with the AI Act's requirements.

The second conformity assessment procedure is the external assessment by notified bodies, outlined in Annex VII. Alternatively, providers may need to undergo an external assessment involving a third-party notified body. This procedure includes a detailed review of the QMS and technical documentation to ensure compliance with the act. This type of conformity assessment procedure can only be conducted by a notified body authorized by a notifying authority, allowing a certification issued by the notified body conducting the

assessment. This certification marks the official recognition that a given AI system meets the requirements provided for high-risk AI systems. Though not officially recognized, AI assurance actions play a crucial role in supporting and preparing for this compliance.

What type of conformity assessment must be conducted?

Conformity assessments are governed by Article 43 of the AI Act. The conformity assessment procedure that must be used is dependent on the type of high-risk AI system.

- → **AI systems used in biometrics.** The provider of the system can choose either the internal or external conformity assessment procedure. However, if the harmonized standards or common specifications are not available or if they are available but only partially complied with, then the provider must follow the external conformity assessment procedure per Article 43(1).

- → **AI systems used in other sectors provided under Annex III.** The provider, in principle, shall follow the conformity assessment procedure based on internal control per Article 43(2).

- → **High-risk AI systems based on union harmonization legislation.** The provider shall follow the relevant conformity assessment procedure as required under those legal acts.

What are harmonized standards?

Harmonized standards are technical standards, and conformity with them triggers a presumption of conformity with the requirements provided under Section 2 of the act to the extent that a given standard covers a requirement provided thereunder. Technical standards are one of the most important practical tools provided under the AI Act but are not yet available.

Only standards issued by the European standardization authorities, which are the European Committee for Standardization, the European Committee for Electrotechnical Standardization and the European Telecommunications Standards Institute, can be harmonized with the AI Act, provided they are issued after following the required procedure. In May 2023, the European Commission issued an implementing decision on standardization requesting the CEN and CENELEC to draft new European standards or European standardization deliverables supporting EU AI policy, as listed in Annex I, by 30 April 2025.

It is important to note, despite their practical value associated with industry practices, International Organization for Standardization and International Electrotechnical Commission standards are not harmonized standards with the AI Act. In other words, compliance with other standards will not automatically denote compliance with the AI Act.

What are common specifications?

Common specifications are tools to aid in compliance with requirements under Section 2 when there is no harmonized standard despite the Commission's request and one will not be published in the Official Journal of the European Union within a reasonable time. In other words, common specifications are temporary substitutions for the harmonized

standards issued by the European Commission rather than EU standardization bodies.

Where is AI assurance in the picture?

While private AI assurance tools do not provide the official conformity stamp, they are valuable in establishing practical trust. The level of trust depends on the credibility and expertise of the firm conducting the assurance. These tools can evaluate an AI system's compliance readiness, identify potential risks and suggest improvements to enhance compliance with the AI Act. Private AI assurance tools or techniques are not official conformity assessment procedures. More specifically, these are neither harmonized standards nor common specifications of the AI Act. However, these tools may significantly facilitate the preparation process for compliance with AI Act requirements or obligations.

There are two main functions a private AI assurance tool can play in the compliance journey of a given AI system with the AI Act.

AI assurance supporting compliance

AI assurance actions can support compliance by internally assessing how well a system or operator is prepared for the official conformity assessment. These private assessments can identify gaps, recommend improvements and enhance the system's readiness for the official procedure.

Complementary nature

While AI assurance tools cannot replace formal conformity assessments made by notified bodies, they can prepare operators for such external conformity assessments or for internal ones by providing additional layers of scrutiny and validation. This creates a practical trust level based on the firm's trustworthiness in conducting the assurance.

Assurance in practice

While private AI assurance tools do not provide the official conformity stamp, they are valuable in establishing practical trust. The level of trust depends on the credibility and expertise of the firm conducting the assurance. These tools can evaluate an AI system's compliance readiness, identify potential risks and suggest improvements to enhance compliance with the AI Act.

Where are general-purpose AI models located in the AI assurance scheme?

General-purpose AI models are governed by Articles 51-55. Unlike high-risk AI systems, general-purpose AI models are not subjected to mandatory conformity assessment procedures. Depending on their functions, private AI assurance tools or mechanisms may facilitate a given general-purpose AI model in achieving compliance with the requirements.

The AI Office is empowered to encourage and facilitate the drawing up of codes of practice at the EU level per Article 56(1). These codes of practice can be relied upon to show compliance with the respective set of obligations until a harmonized standard is published. Providers of a general-purpose AI model that do not adhere to an approved code of practice or comply with a published harmonized standard must demonstrate alternative adequate means of compliance for assessment. Here, private assurance tools may qualify as alternative adequate means of compliance with the act.

Conclusion

AI assurance is an essential part of AI governance and must be understood as a concept that is distinct from compliance for the purposes of the AI Act. While compliance focuses on meeting established standards through formal conformity assessments, assurance offers a broader and ongoing evaluation to build trust and ensure long-term reliability. Together, they contribute to a safe and trustworthy AI market, aligning with the goals of the AI Act. AI assurance tools and mechanisms may facilitate or support compliance with the AI Act or function as alternative means of compliance for the purposes of the general-purpose AI models. However, as notified bodies do not provide the tools and mechanisms for compliance, they cannot officially recognize compliance with the AI Act and will trigger legal implications and presumptions.

Published September 2024

Post-market monitoring, information sharing and enforcement

By Shima Abbady and Puck van den Bosch

Chapter IX of the EU Artificial Intelligence Act includes post-market monitoring, information sharing and enforcement provisions. Readers familiar with the EU General Data Protection Regulation will see some similarities but mostly important differences, as the AI Act is primarily a product safety regulation heavily inspired by the structure of product safety laws in the New Legislative Framework, such as the Medical Device Regulation.

Post-market monitoring obligations under the AI Act

As a regulation primarily focused on product safety, the AI Act includes ex-ante and ex-post obligations. The rationale is to ensure continuous compliance of AI systems with the AI Act throughout their life cycles, which is important as many AI systems change after implementation, such as through continuous learning after deployment. This can make it difficult to comprehensively foresee all risks the system may present in practice when it is developed.

Article 72 of the act requires providers of high-risk AI systems to collect and review experience gained from using their AI systems after they have been placed on the market or put into service. Such information may sometimes be provided by deployers but can also be collected through alternative sources, such as affected persons or competent authorities. The purpose of these post-market obligations is to ensure AI systems continuously remain compliant after the provider places them on the market, with the requirements that apply to high-risk AI systems under Section 2 of Chapter III. Providers can, and should, use the findings to improve their systems, as well as the design and development process, and take any possible corrective action when necessary.

Article 72 notes the post-market monitoring system should be based on a post-market monitoring plan, which should be part of system's technical documentation and that providers are obliged to keep up to date throughout its life cycle. To assist providers with setting up such a plan, the AI Act requires the European Commission to adopt an implementing act with detailed provisions

that establish a template for the post-market monitoring plan by 2 Feb. 2026.

Information obligations for serious incidents

Article 73 obliges providers of high-risk AI systems to report serious incidents to the market surveillance authorities of the member states where the incident occurred. Procedures for such incident notification should be included in the AI system's quality management system, per Article 17(1)(i). In principle, deployers of high-risk AI systems should immediately inform the system's provider of any serious incidents identified. If they cannot reach the provider, they should instead follow the procedure in Article 73 and notify the market surveillance authority, per Article 26(5).

It is important to note infringements of fundamental rights are viewed as serious incidents, which is cause for operators of high-risk systems to pay close attention. The fundamental rights mentioned here are primarily those included in the Charter of Fundamental Rights of the European Union, which includes a long list of rights ranging from traditional civil rights, such as the right to life, to rights that may often be overlooked, such as the right to consumer protection. On the other hand, a serious incident only occurs when it leads to a breach, not when this consequence is a mere possibility.

Unlike the GDPR, the AI Act does not provide for a one-stop-shop system. As such, providers may not have the option of reporting solely to a lead supervisory authority when the AI system is deployed in multiple member states. If a serious incident affects multiple member states, providers must notify the market surveillance authority in each member state where the AI system is available.

In principle, providers must report serious incidents immediately but no later than 15 days after establishing a link between the incident and the AI system or a reasonable likelihood of such a link. Similar to the GDPR, an interim notification may be sent instead if a complete report is unavailable at the time of initial reporting. The act is unclear about whether providers can submit multiple interim reports before the final report. It also does not specify a deadline for filing the final report. Per Article 73(7), the Commission must publish guidance to facilitate compliance on reporting serious incidents at the latest 12 months after the act enters into force, by 2 Aug. 2025, which could clarify this issue.

After filing the report, providers must perform the necessary investigations of the serious incident and the AI system involved. This includes performing a risk assessment and taking any necessary corrective actions. This investigation cannot include altering the AI system in a way that may affect any subsequent evaluation of the causes of the incident before informing the competent authorities of such action.

After receiving a notification, the market surveillance authority will inform the relevant national public authorities or bodies and, within seven days, take appropriate measures. When there are no other effective means to eliminate the serious risk, the authority can withdraw or recall the AI system or prohibit it from being made available on the market. The competent authorities will also notify the European Commission. If the serious incident involves infringing fundamental rights, the market

surveillance authority or authorities must also inform the national fundamental rights authority or authorities.

Exemptions from notification apply when the AI system is subject to the Medical Device Regulation or the In Vitro Diagnostic Medical Device Regulation. In such cases, notification under the AI Act must only be done when the incident concerns an infringement of fundamental rights, e.g., the right to be free from discrimination, which is not covered by these regulations.

Enforcement: A fragmented surveillance landscape

The AI Act's enforcement will differ from the GDPR's. While data protection authorities will likely play an important supervisory role, the enforcement of the AI Act will involve a number of other authorities at both the national and EU levels. Notably, there is no one-stop-shop system, which means organizations do not have the option to appoint a single lead supervisory authority for their businesses. This does not come as a surprise entirely, as the one-stop-shop system is not typically applied in product safety regulation. However, it does mean organizations may face a complex supervisory landscape.

Section 3 of Chapter IX lays down the rules for enforcement by setting defined rules on the competence of the different national competent authorities. As a preset, Regulation (EU) 2019/1020 is declared applicable to AI systems covered by the AI Act, which means all provisions apply mutatis mutandis to the market surveillance of AI systems. Member states can designate more than one market surveillance authority for the surveillance of the AI Act, provided their respective duties are clearly defined, and appropriate communication and coordination mechanisms are in place. It appears most member states will use the option to appoint multiple market surveillance authorities and, additionally, multiple sector-specific supervisory authorities.

Market surveillance authorities will be responsible for the supervision and enforcement of the AI Act. Among other things, they are tasked with overseeing the testing of AI systems in real-world conditions in accordance with the AI Act. They also conduct evaluations of AI systems that potentially pose risks to people's health, safety or fundamental rights. Market surveillance authorities are also responsible for handling serious incident notifications. They have all the powers laid out in Article 14 of the Market Surveillance Regulation, which includes the powers to carry out unannounced on-site inspections, acquire product samples, reverse-engineer them, identify noncompliance, obtain evidence, recall AI systems and impose penalties. Additionally, Articles 74(13) and 74(14) provide for the powers to be granted full access by providers to the documentation as well as the training, validation and testing datasets used for the development of high-risk AI systems and, under certain conditions, to the source code of the high-risk AI system.

For the most part, member states are free to appoint the market surveillance authorities of their choice. However, Article 74 does designate specific authorities for certain areas of surveillance. The market surveillance authorities set out for AI systems regulated by the directives and regulations in Section A of Annex I, also referred to as the New Legislative Framework, will generally be competent under the AI Act. Annex I(A) covers a wide array of

products, including machinery, toys, radio equipment, in vitro medical devices, two- or three-wheel vehicles and quadricycles, and motor vehicles.

Operators of high-risk AI systems that fall within this scope will generally not have to deal with additional market surveillance authorities. The existing procedures, e.g., dealing with risks and formal noncompliance pursuant to these regulations, will often apply instead of those pursuant to the AI Act. For AI systems placed on the market, put into service or used by financial institutions, the market surveillance authorities, under applicable financial services law, will generally act as market surveillance authorities insofar as a direct connection exists with regulated financial services. Member states can appoint a different market surveillance authority if appropriate and only insofar as coordination is ensured.

Additionally, Article 74(8) appoints the national authorities, designated through either the GDPR or Law Enforcement Directive, usually the national DPA in both cases, as the competent market surveillance authorities for the high-risk AI systems in the following areas:

- → Law enforcement under Annex III, point 6.
- → Migration, asylum and border control management per Annex III, point 7.
- → Administration of justice and democratic processes under Annex III, point 8.
- → Biometrics under Annex III, point 1, but only insofar as they are also used in any of the above areas.

Member states are not allowed to designate any authority other than those appointed based on the GDPR or Law Enforcement Directive.

Besides the foregoing, other competent national authorities can be appointed because they already have competence at a certain level or regarding specific topics, including having a preexisting mandate, such as if they are already national cybersecurity supervisors, or being allotted competence under Article 77 because they protect fundamental rights. Overall, the AI Act will often present a fragmented supervisory landscape, which will require coordination between different authorities to function properly.

At the EU level, however, the AI Act takes a centralized approach. It allocates supervisory powers to two entities that will function as one-stop shops: the European Data Protection Supervisor and the EU AI Office, which was established as a part of the European Commission in May 2024. Pursuant to Article 74(9), the EDPS will be the market surveillance authority for EU institutions, bodies, offices or agencies without room for derogation. Article 88 designates the AI Office as the competent authority for monitoring and supervising general-purpose AI models. Insofar as AI systems are based on general-purpose AI models, the AI Office will also have the power to monitor and supervise compliance, provided the same provider develops the model and the system. The AI Office can monitor compliance, for instance by requesting documentation or conducting evaluations, but can also act based on complaints by downstream providers or alerts of systemic risks by the Scientific Panel of Independent Experts. Aside from its surveillance duties, the AI Office is set to

focus on encouraging and facilitating codes of practice to contribute to the proper application of the AI Act to general-purpose AI models, provide coordination for joint investigations between market surveillance authorities from different member states, and work closely with the European AI Board to support national competent authorities in the establishment and development of regulatory sandboxes.

Few remedies for affected persons

Unlike the GDPR, the AI Act does not offer involved persons many remedies to invoke when providers or deployers have breached an obligation to their detriment. Essentially, the act offers only two rights to affected persons: the right to lodge a complaint with the relevant market surveillance authority and the right to receive an explanation of individual decision-making, which is mainly based on the output of a high-risk AI system.

The right to lodge a complaint can be found in Article 85 of the act and can be exercised by both natural and legal persons. If a person has grounds to consider that there has been an infringement of the act, they can submit their reasoned complaint to the relevant market surveillance authority. The authority will use those complaints for the purpose of conducting market surveillance activities. Authorities can choose to handle complaints according to their own established procedures. A similar right is provided to downstream providers of general-purpose AI models, i.e., parties that use such models to build AI systems, per Article 89 of the act. Downstream providers can submit duly reasoned complaints to the AI Office when they believe a general-purpose AI provider has infringed the AI Act.

The right to an explanation of individual decision-making can be found in Article 86. While reminiscent of the GDPR's right to not be subject to automated decision-making, the right established in the AI Act does not generally prohibit automated decisions based on AI system outputs but instead provides affected individuals the right to an individualized explanation. This right can be invoked whether the decision was automated or nonautomated within the meaning of GDPR Article 22.

Any affected person subject to a decision made by a deployer on the basis of the output from a high-risk AI system, as listed in Annex III, that produces legal effects or similarly significantly affects that person in a way they consider to have an adverse impact on their health, safety or fundamental rights, has the right to obtain clear and meaningful explanations of the AI system's role in the decision-making procedure and the main elements of the decision from the deployer. Such an explanation should be clear and meaningful and should provide a basis on which the affected persons are able to exercise their rights. Although the provision does not explicitly state whether it applies solely to natural or legal persons, it seems likely that the right extends to both. The right to explanation does not apply, likely for security reasons, if the AI system in question is intended to be used as a safety component in the management and operation of critical infrastructure.

The act does not offer a right to a specific remedy, such as the right to compensation in Article 82 of the GDPR. However, it is worth noting individuals can rely on other regulations, such as the GDPR and liability laws, to address any harm caused by AI systems. The EU is currently working on an

AI Liability Directive to establish more effective means for individuals seeking compensation for damages caused by AI products. If adopted, this directive will make it easier for affected persons to recover damage they suffer due to the deployment of an AI system.

Fines

The rules surrounding penalties are relatively similar to those of the GDPR. Member states must lay down their own rules on enforcement measures, which must be effective, proportionate and dissuasive, and should take into account the Commission's guidelines once adopted.

Under Article 99, the maximum fine amounts to 35 million euros or 7% of the worldwide annual turnover, whichever is higher. This maximum amount applies only to breaches of Article 5, i.e., placing prohibited AI systems on the market or putting them into service. For most other breaches of the AI Act, the maximum fine amounts to 15 million euros or 3% of the worldwide annual turnover. An additional category of fines, with a maximum of 7.5 million euros or 1% of the worldwide annual turnover, is introduced for supplying incorrect, incomplete or misleading information to notified bodies or national competent authorities. This is important for providers and deployers to consider when reporting a serious incident to the market surveillance authority or when requested to share certain information during an investigation. Article 99 further sums up a set of circumstances, similar to those set out in the GDPR, that authorities need to consider when deciding whether to impose an administrative fine and when deciding on the amount of the fine.

The AI Act also contains specific provisions for fines for providers of general-purpose AI models. The Commission can fine these providers up to 15 million euros or 3% of their worldwide annual turnover, if it finds the provider intentionally or negligently:

- → Infringed upon 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.
- → Failed to provide the Commission access to the general-purpose AI model, either with or without systemic risk, to conduct an evaluation pursuant to Article 92.

Just like those applicable to high-risk AI systems, these fines must be effective, proportionate and dissuasive. If a general-purpose AI provider decides to challenge the fine, they will need to turn to the Court of Justice of the European Union, which has unlimited jurisdiction to review the Commission's fining decisions and may cancel, reduce or increase the fine imposed.

Published October 2024

Regulatory implementation and application alongside EU digital strategy

By Isabelle Roccia and Claude-Étienne Armingaud

Launched in 2015, the EU's Digital Single Market Strategy aimed to foster the digital harmonization between the EU member states and contribute to economic growth, boosting jobs, competition, investment and innovation in the EU.

The EU AI Act characterizes a fundamental element of this strategy. By adopting the first general-purpose regulation of artificial intelligence in the world, Brussels sent a global message to all stakeholders, in the EU and abroad, that they need to pay attention to the AI discussion happening in Europe.

The AI Act achieves a delicate balancing act between the specifics, including generative AI, systemic models and computing power threshold, and its general risk-based approach. To do so, the act includes a tiered implementation over a three-year period and a flexible possibility to revise some of the more factual elements that would be prone to rapid obsolescence, such as updating the threshold of the floating point operations per second — a measurement of the performance of a computer for general-purpose AI models presumed to have high impact capabilities. At the same time, the plurality of stakeholders involved in the interpretation of the act and its interplay with other adopted, currently in discussion or yet-to-come regulations will require careful monitoring by the impacted players in the AI ecosystems.

The EU digital strategy and digital decade

The 2015 Digital Single Market Strategy for Europe foresaw a potential 250 billion euros in generated value and called for a "vibrant knowledge-based society." To implement that vision, the European Commission revealed an ambitious legislative program, which included reforming the EU's telecommunications and copyright legislation and simplifying consumer rules for online and digital purchases, in addition to putting the General Data Protection Regulation into force.

To further this initial ambition, given the ever-so-quick evolution of emerging technologies,

the Commission proposed its Path to the Digital Decade in September 2021, followed in December 2022 by the European Declaration on Digital Rights and Principles.

These initiatives not only aimed to modernize the EU regulatory landscape but also to create a stance for Europe by setting up a common corpus of EU democratic values in the digital sphere and ensuring the value generated by this dematerialized sphere benefited Europe.

To support this effort, significant EU funding has also been made available to foster the digital transformation, in particular through the Recovery and Resilience Facility at 150 billion euros, DIGITAL Europe at 7.9 billion euros and Connecting Europe Facility 2 Digital at 1.7 billion euros.

While several aspects of this digital strategy appeared as a logical continuation of existing process, e.g. digital resilience in the financial or other critical sectors, see the Directive on Security of Network and Information Systems and Digital Operational Resilience Act below, the topic of AI quickly arose, almost unannounced.

Once generative AI became publicly available, the media coverage of the promises of AI and its rapid adoption led to the full spectrum of reactions from doomsday sayers to utopians.

Although it was a late guest to the EU digital roadmap, the AI Act went through an accelerated adoption process alongside other texts that were previously initiated. This article aims to analyze the regulatory implementation of the AI Act, notably its interplay with these other regulatory frameworks.

A macro view of the AI Act with other elements of the EU digital strategy

While the AI Act aims to regulate AI generally, its ambition was never to regulate exclusively. Indeed, the ubiquity of AI systems facilitates their inclusion in other products and services that are subject to other regulatory frameworks.

This means compliance with the AI Act is incumbent on compliance with other EU regulations, whether they are technology-neutral cross-sector regulations like the GDPR or sector-specific regulations like the DORA. These additional compliance requirements depend on the specific use case in which a given AI system is deployed.

Data protection

The AI Act and GDPR are part of the broader regulatory landscape designed to govern digital technologies and protect individuals in the digital age. While focusing on different aspects of digital technology and the use of both personal and nonpersonal data, these two pieces of regulation interact closely and share common goals. The eagerness with which some EU data protection authorities leveraged the GDPR, e.g., to tackle AI-related investigations and produce guidance, before the adoption of the AI Act illustrates the interplay and partial overlap between these frameworks.

Principles

Many of the foundational principles that inspired the AI Act are common to data protection, including privacy and data governance, transparency and accountability. However, there is undeniable friction between some of the GDPR innate governing principles and the mere nature of AI technology. Data minimization is perhaps the most obvious.

Complementarity

Not all AI systems use personal data as part of their functionalities. Consequently, the GDPR may not always be a relevant framework. However, the massive ensembles of data processing by large language models, especially in the absence of curation, e.g., through web scraping, makes it more than likely that the GDPR will be relevant, as recently demonstrated by the position on LLMs taken by Hamburg's data protection authority, the Commissioner for Data Protection and Freedom of Information. Similarly, while the GDPR does not focus on AI, its Article 22 provisions pertaining to automated decision-making highlight the interplay, overlap, overall complementarity and, at times, conflict between the two. Overall, the GDPR is directly referenced 30 times in the AI Act, far more than any other EU regulation.

Risk-based approach

Both the GDPR and the AI Act employ a risk-based approach, but they categorize and handle risks differently. The GDPR categorizes data processing activities based on the level of risk to the data subjects' rights and freedoms, while the AI Act categorizes AI systems based on the level of risk they pose to safety, fundamental rights and other public interests. While the two risk-based approaches often overlap, and the risk-based approach under the GDPR has been put in question, they may also add to one another.

Impact assessments

Under the GDPR, data protection impact assessments are mandatory for high-risk data processing activities. On the other hand, the AI Act also requires impact assessments but focuses on fundamental rights and the ethical use of AI, evaluating issues such as bias, discrimination and potential harm. Once again, while they may partially overlap in scope and purpose, stakeholders will need to devise templates to address all facets. Ideally, the stakeholders responsible for drafting, implementing and maintaining those impact assessments will be able to leverage their DPIAs to meet some of the fundamental rights impact assessment requirements and either be on the same team or closely work together to avoid discrepancies in the documentation.

Supervision and enforcement

Both the AI Act and GDPR provide for robust supervision and enforcement mechanisms. The AI Act creates new bodies, including the AI office and AI Board, and will rely on a net of national authorities. While, under the GDPR, DPAs have been well established for years in each EU member state, the relevant authorities under the AI Act are still debated, which may ultimately lead to divergences in interpretation and enforcement.

Governance

The intricate nature of the two regulations will make for an even more complex framework. However, it also means many organizations will be able to significantly leverage the privacy tools, processes, structures and culture already in place to inform and build their AI governance.

Cybersecurity

The EU's regulatory framework for cybersecurity, including the DORA, the not-yet-adopted Cyber Resilience Act, the revised NIS2 Directive and the Critical Entities Resilience Directive, along with the AI Act, form a comprehensive strategy to address different

aspects of the EU's expectations for digital security and resilience. While each of these pieces has its own focus area, be it specific or general, together they have the overarching goal of creating a safer digital environment within the EU.

- → **DORA:** This aims to ensure the EU financial sector can maintain operational resilience with a particular focus on information and communications technology risk management. It sets out requirements for financial entities to establish and maintain preventive measures, detection mechanisms, and strategies to respond to and recover from ICT-related disruptions and threats.

- → **CRA:** This aims to encourage a life-cycle approach to connected devices, ensure they are placed on the market with fewer vulnerabilities, and enable users to take cybersecurity into account when selecting and using connected devices.

- → **NIS2 Directive:** This updates the scope of the original Network and Information Security Directive by expanding the security and notification requirements to more sectors and types of entities, raising the bar for cybersecurity standards, and strengthening national cybersecurity capabilities. It covers a broad range of critical sectors beyond the financial industry.

Complementary objectives

Each piece of the framework shares the common objective of mitigating risks associated with digital technologies. Where the AI Act focuses on risks specifically associated with AI systems, DORA, CRA and NIS2 target the broader digital ecosystem's stability and security.

Risk management

All four pieces of the framework adopt a risk-based approach, alongside accountability frameworks. Stakeholders will need to demonstrate that they not only mapped the actual or potential risks, including AI, associated to their ICT, infrastructure, products and services as relevant, but that the relevant mitigation efforts have been implemented, notably in view of the evolution of technological progress and the state of the art. In addition, similar to the AI Act, the CRA includes obligations to include cybersecurity risk assessments in the technical documentation of new connected devices placed on the market.

Reporting obligations

All pieces of the framework include obligations to report incidents occurring on the platform and/or device to the relevant authorities. When more than one framework applies, stakeholders will need to consider all reporting obligations. Ideally, the authorities responsible for enforcing the AI Act will coordinate with those responsible for the DORA, CRA and NIS2, especially when dealing with AI systems that fall under the critical infrastructure categories. This will be a familiar notion, as incident notification requirements must be considered under NIS2 and the GDPR among other laws.

Operational resilience

AI systems, especially those used within critical infrastructures, need to adhere to the resilience standards outlined in the DORA and NIS2. This means AI system developers and deployers must ensure their systems can withstand, respond to and recover from cyber threats.

In essence, the AI Act, DORA, CRA and NIS2 form a comprehensive approach to safeguarding

the EU's digital ecosystem. They are different pieces of the same puzzle, with each regulation targeting specific challenges but ultimately contributing to the resilience, security and trustworthy adoption of digital technologies, including AI, across the EU.

The harmonized application of these regulations is crucial for ensuring the consistency and effectiveness of the digital single market's security, whether by the relevant stakeholders to not duplicate the compliance effort, or the relevant authorities to ensure enforcement actions are coherent. The failure of a coordinated implementation regime would lead to discrepancies and lack of foreseeability by the stakeholders. Technology developments and the evolution of the threat landscape will also be implementation challenges for organizations. This landscape also leaves some room for organizations to leverage AI technology to strengthen their cybersecurity postures.

The AI Act is expected to work in tandem with the GDPR and other digital regulations to create a comprehensive and cohesive framework for digital technology in the EU. In addition, its compliance mechanisms and enforcement will likely build on the foundational doctrines and interpretations developed over the past years. Stakeholders will need to maintain that broad bird's-eye view of the EU regulatory landscape, as well as any changes in the implementation of its components to ensure continued compliance.

Copyright

The EU last updated its copyright rules in its 2019 Digital Single Market Directive, reflecting the state of the art at the time, so minimal provisions are relevant for AI and machine learning. The directive's Article 4 on text and data mining creates an exception to copyright for text and data mining purposes. In fact, copyright appeared late into the AI Act negotiations at the request of the European Parliament, as co-legislators were zeroing in on obligations for general-purpose AI models. The final text primarily draws from EU copyright law.

Article 53 of the AI Act requires providers of general-purpose AI models to put policies in place to comply with EU copyright law, for example to make sure the training data they use respects copyright. They also need to comply with the reservation of rights pertaining to the TDM exception in the Copyright Directive and seek authorization from the copyright holder when needed.

The same article also requires general-purpose AI model providers to "draw up and make publicly available a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office."

Putting these requirements in practice in the context of the AI Act will not be straightforward and the AI Office is expected to provide useful guidance to stakeholders in that regard, including to clarify the notion of a "sufficiently detailed summary."

A currently incomplete map of requirements

In addition to the expected guidelines and delegated acts, standards are expected to play a key role in stakeholders' compliance effort, notably to benefit from a presumption of conformity, as in Recital 117 and Article 40 et. seq. of the AI Act.

While the European standardization organizations, comprising the European Committee for Standardization, with the European Electrotechnical Committee for Standardization and the European Telecommunications Standards Institute, are currently working on various sets of standards, the official mandate to adopt harmonized standards may not be issued prior to the publication of the AI Act in the Official Journal of the EU. As such, the publication of finalized harmonized standards will be adopted after stakeholders' compliance efforts have started.

Stakeholders will therefore need to pay close attention to the development and publication of these standards. They should prepare their compliance in advance, the case may be on the basis of the published draft, as they will have a narrow window to ensure alignment with technical specifications and complete their conformity assessments.

A growing risk of divergent interpretations

The AI Act includes compliance requirements at both the pre- and post-market stages of AI system deployment. Its enforcement will be entrusted to one notifying authority and one market surveillance authority in each member state per Article 70 of the AI Act. While the resulting designation may target the same authority, this will not always be the case.

In addition, over the past couple of years, several DPAs in big member states have actively leveraged their GDPR responsibilities to assert their expertise in AI systems and relevance in supervising and enforcing the AI Act. All DPAs expect to have a seat at the table, and some have advocated very strongly to become the lead authority.

Each member state retains full control of these designations, still pending in a majority of countries. The close links between the AI Act and the Market Surveillance Regulation no. 2019/1020, see AI Act Article 74, may tip the balance in favor of the well-established member state infrastructure of market surveillance authorities already in charge of the post-market monitoring regime for products in the EU.

The designation of authorities is not straightforward as neither MSAs, DPAs nor any other existing authority would be the perfect blend. For example, one may argue DPAs are not the most relevant authority because AI may not always involve personal data processing activities. Some member states, like Spain, may choose to create a new authority from scratch.

As a result, and despite the tempering function of the EU AI Board, interpretations of key concepts under the AI Act and its enforcement may follow diverging regime and the regulatory implementation may include discrepancies from one member state to the other.

The AI Act created the AI Office, which will advise and assist the European Commission and EU member states to strive for an EU-wide harmonization as part of its mission. Yet, the AI Act builds on a complex matrix of stakeholders that each bring a variety of expertise, cultural and historical differences, which may be challenging to reconcile and harmonize.

The potentially fragmented interpretation could also lead to more stringent requirements bearing on certain stakeholders in certain jurisdictions.

The look ahead

Following the 12 July 2024 publication of the AI Act, the Commission circulated an updated version of the AI Liability Directive that considers the final content of the AI Act, which aims to provide compensation to victims of damage caused by AI. According to Member of the European Parliament and AI Liability Directive Rapporteur Axel Voss, the recently updated Product Liability Directive contains enough loopholes to justify continued work on the AI Liability Directive. This was reiterated by the Parliament's research service in a study that argues the scope of the AILD proposal should extend to include general-purpose and other high-impact AI systems, as well as software.

In its latest version of the AI Liability Directive, the Commission mostly changed the text's wording to match the AI Act's. However, the Commission's changes to Article 4 of the directive increases the potential responsibility of companies deploying AI systems. As it is currently redrafted, this Article 4 would result in the presumption that companies are liable for damage caused if they do not "monitor the operation of the AI system or, where appropriate, suspend (its) use" or use "sufficiently representative" input data.

While compliance with the AI Act should minimize the risk of exposure to liability under the AI Liability Directive, this companion piece will provide individuals with recourse to compensation for the potential damage resulting from the deployment of AI, as opposed to the regulatory fines under the AI Act. This framework would bring more clarity than stakeholders have seen until now under the GDPR, the enforcement of which remains under discussion before the courts, notably for nonmaterial damages.

Conclusion: The need for self-determination of ecosystems

With so many unknowns in the compliance equation, the AI Act may not provide the stakeholders with the expected regulatory foreseeability, which will be the key to developing competitive AI systems and preserving the EU's fundamental democratic values.

In addition, while the EU welcomes input from the stakeholders when developing normative elements, the compromises that must be reached for a baseline regulatory implementation bearing on all stakeholders may not be conducive of accounting for the specific factors of certain ecosystems.

Yet, like the GDPR, the AI Act may retain an ace up its sleeve with codes of practice and codes of conduct.

In the meantime, stakeholders were also invited by the Commission to provide their input on AI, notably through its:

- Directorate-General for Health and Food Safety, which opened a survey on the deployment of AI in health care.
- Directorate-General for Financial Stability, Financial Services and Capital Markets Union, which ran a consultation to gather input from all financial services stakeholders, including companies and consumer associations. Responses can be submitted until 13 Sept. The consultation was designed for respondents developing or planning to develop or use AI applications in financial services. In particular, the DG FISMA aimed to receive views from financial firms that provide or deploy AI systems.

Published November 2024

Leveraging GDPR compliance

By Nils Hullen

The EU AI Act mentions the EU General Data Protection Regulation, Regulation (EU) 2016/679, more than 30 times throughout its recitals and articles, which define the European framework for the development and deployment of high-risk AI systems and general-purpose AI models.

This does not come as a surprise, as many AI models are trained with datasets, including personal data, and most AI systems are used by humans who can be identified by their usernames or other log-in credentials.

In addition, both regulations aim to protect the fundamental rights of individuals and the responsible use of data, as outlined in Recital 10 of the AI Act. The GDPR safeguards the right to the protection of personal data in particular. The AI Act focuses primarily on the health and safety of individuals, as well as other fundamental rights protecting democracy, the rule of law or the environment.

Personal data and AI

The AI Act includes specific rules that cover biometric data, profiling and automated decision-making, which are also within the scope of the GDPR. Furthermore, the AI Act clarifies the GDPR always applies when personal data is processed. These regular processing scenarios are also subject to GDPR rules, when the processing takes place within its territorial scope per Article 2 and when the processed data is personal, meaning it relates to the data subject, an identified or identifiable natural person, per Article 4.

If personal data is used to train an AI model to improve a picture uploaded to an online photo editor, or simply because a user logs onto the AI system with their name and email, the GDPR rules need to be followed as usual. First and foremost, that means processing personal data requires a legal basis, according to GDPR Article 6. In the context of model training and the deployment of AI systems, there are three main legal grounds to consider: the legitimate interests pursued by the controller or by a third party, contractual necessity, and the data subject's consent. Also, other legal

grounds can justify processing personal data in specific circumstances, such as when the "vital interests" of a data subject are protected in emergency situations.

The AI Act specifically addresses the use of sensitive personal data or "'special categories of personal data," in the language of GDPR Article 9. Article 10 of the AI Act provides legal grounds for processing these special categories of sensitive data, specifically and exclusively for bias detection and correction in relation to high-risk AI systems. However, this exception only applies if certain conditions are met. Among others, the use of other nonsensitive data, including synthetic or anonymized data, is not sufficient to ensure bias is appropriately addressed in high-risk AI systems. The AI Act also requires sensitive personal data used for bias mitigation to be safeguarded by technical measures, including the pseudonymization of sensitive data, to limit the reuse of the data and, more broadly, to enhance security and privacy protection.

Privacy-enhancing technologies are important tools to solve the potential conflict between the GDPR's data minimization principle and the requirement to process large datasets, which can help ensure AI systems make fair and accurate assumptions. Various PETs, including anonymization, synthetic data, federated learning and fully homomorphic encryption, also available as open source or "as a service," can help unlock the value of personal data in the AI context in compliance with the GDPR rules.

Common principles and approaches

The GDPR kicks in only when personal data is processed, regardless of whether AI is involved. In contrast, the AI Act applies irrespective of whether personal or nonpersonal data is used. Nevertheless, both regulations share some common principles and approaches to implementing their respective provisions, and both are are well known to most privacy professionals. Key principles like accountability, fairness, transparency, accuracy, storage limitation, integrity and confidentiality, which are fundamental for processing personal data under Article 5 of the GDPR, are also enshrined in the AI Act and, as such, are not a novelty to companies processing personal information.

Accountability

The GDPR requires organizations processing personal data to fulfill the applicable requirements of the EU data protection framework and to demonstrate their compliance with the law. To fulfill their accountability obligations under Article 30 of the GDPR, controllers and processors of personal data must keep detailed documentation of their respective processing activities and make them available to data protection authorities upon request, among other things. Accountability is also a fundamental principle of the AI Act, incorporated in various provisions. For example, providers of high-risk AI systems are responsible for ensuring their products adhere to the relevant provisions of the AI Act and for documenting their compliance in "a systematic and orderly manner, in written policies, procedures and instructions" per AI Act Article 17. Furthermore, they are required to keep various technical and organizational documents updated and at hand for requests by authorities per Article 18.

Fairness

Fairness, and with it, nondiscrimination, is one of the fundamental AI ethics principles

incorporated into Recital 27 of the AI Act. It is reflected by the obligations of providers to test high-risk AI systems in Article 9, examine datasets for possible biases in Article 10, ensure high-risk AI systems meet an adequate level of accuracy in Article 15 and take corrective actions if necessary in Article 20. Correspondingly, per Article 26, deployers of high-risk AI systems must ensure input data is relevant and sufficiently representative given the intended purpose of the high-risk AI system. They need to ensure they do not over-rely on the output produced by the AI system — automation bias — and conduct, in some instances, fundamental rights impact assessments per Article 27 to avoid unfair decisions involving AI systems in high-risk use cases. Within the realm of the GDPR, fairness, along with lawfulness and transparency, is one of the guiding principles for data processing. It is enshrined in information requirements in GDPR Articles 12-14 and in data subject rights, such as the right to rectify inaccurate data in Article 16 and the right not to be subject to automated decision-making in Article 22.

Human oversight

Human oversight is also one of the fundamental principles of AI ethics and a specific requirement of the AI Act. According to Article 14, high-risk AI systems must be designed to be effectively overseen by "natural persons," i.e., humans. This corresponds with the obligation of the organization deploying the system to assign human oversight to a person who has the competence, training and authority to fulfill this task, as well as the necessary organizational support as outlined in Article 26. This aspect is not new for privacy pros. Under Articles 37-39 of the GDPR, controllers and processors may need to appoint data processing officers. These are dedicated and skilled people with access to sufficient resources who oversee the data processing activities within the organization. Also, if individuals are subject to decisions based solely on automated processing that produce legal effects or similarly significantly affect them, they have the right to contest the decision and to obtain human intervention and oversight from the data controller per GDPR Article 22.

Data subject and AI Act rights

Handling data subject rights requests is an essential part of any privacy compliance program. For example, under the GDPR, data controllers must inform data subjects about the personal data they process, correct and delete data if necessary, or provide them with a copy of the data to transfer them to another controller. All data subject rights apply when personal information is processed in the context of an AI system. Article 85 of the AI Act establishes only a few specific rights related to the nature of product safety law, such as the right for any natural or legal person to lodge a complaint with a market surveillance authority. Downstream providers using general-purpose AI models can lodge a complaint with the European Commission's AI office, which monitors compliance with the rules for such AI models, per Article 89. And, last but not least, AI Act Article 86 contains the right of explanation to individual decision-making. This right only applies to certain high-risk AI use cases. Hence, it is narrower than the comparable data subject right enshrined in Article 22 of the GDPR. It only applies to the extent that the right is not otherwise provided for under European law, including the GDPR.

Impact Assessments

Privacy pros are familiar with privacy impact assessments or, in terms of GDPR Article 35, data protection impact assessments. The AI

Act implements a similar instrument, the fundamental rights impact assessment, in Article 27. The FRIA is limited to specific high-risk AI use cases, such as when public sector entities plan to deploy high-risk AI systems or when AI systems are used to evaluate a person's creditworthiness. Nevertheless, the underlying principle is similar to the DPIA. Hence, the AI Act specifically states the DPIA required by the GDPR can serve as a basis and can be complemented by additional AI-related aspects, which would result in the required FRIA.

Breach and incident notifications

Last but not least, breach notifications are part of any privacy management system to ensure personal data breaches are reported to DPAs within 72 hours, per Article 33 of the GDPR. Following a similar mechanism, details like timelines vary, so providers of high-risk AI systems must report serious incidents to the market surveillance authorities. Providers must implement a communication and investigation process in either case to report data breaches or AI incidents to the competent authorities.

AI and privacy compliance approaches

Compliance with privacy laws requires a systematic approach that stretches across all levels of an organization, large or small. With the applicability of the GDPR and other similar privacy laws, many companies implemented global privacy management systems to cope with the rapidly expanding regulatory landscape and the increasing amount of personal and nonpersonal data utilized in a business context. In many cases, an existing privacy management or, more broadly, a governance, risk and compliance system is the ideal starting point to tackle the AI-related requirements stemming from the AI Act and the other AI-adjacent laws that will emerge over the coming months and years.

A core element of each privacy management system is an inventory of data processing activities, flows and applications using personal data. Organizations can leverage this inventory to include AI models, applications and the data used to develop and operate AI systems. Such an integrated governance system can capture, integrate and make transparent the metadata related to the entire AI life cycle from design to deployment to everyday use, as well as assess and monitor the risks related to the processing of sensitive personal data and the specific risks associated with AI models, such as general purpose AI models with systemic risks, per AI Act Article 51, or high-risk AI systems.

Privacy management systems are often the gateway to relevant documents, such as data processing agreements, vendor contracts, consent forms, records of processing activities and other key performance indicators, like the number of registered inventory assets, response time to data subject requests, number of DPIAs or privacy training completion rates.

For compliance with the AI Act, and AI governance in general, these features can also be used to help create AI fact sheets, establish user information, or collect and analyze the behavior of AI systems, providing relevant information and KPIs in dashboard views.

While existing privacy management approaches are a good starting place, AI governance has unique challenges. The interplay between personal and nonpersonal data, AI models and AI systems is much more dynamic and complex compared to the normal privacy environment. Also, the deep technical expertise of data engineers and data scientists is required to fulfill certain requirements of the AI Act. Automation is a key component in helping manage that complexity and apply technical skills at scale. AI and data governance platforms can provide the tools needed for an integrated and continuous compliance approach, which supports organizations in coping with the plethora of new privacy, data governance and AI regulations, such as the AI Act.

Contact

Joe Jones
Director of Research and Insights, IAPP
jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media

Published November 2024.