Chapter Seven

EU Regulatory Trends Impacting Companies Using Third-Party AI Tools

Written by

WILSON SONSINI

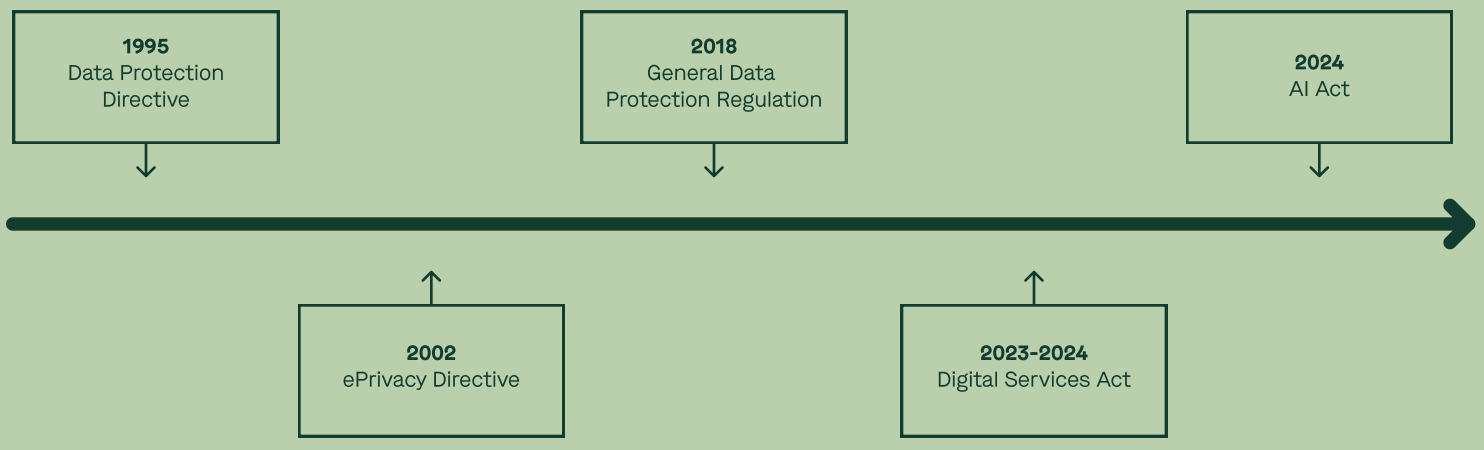
Authors: Laura De Boel and Marie Catherine Ducharme

Table of Contents

Overview

The AI Act: The Latest Addition to a Complex Landscape

Europe has been regulating the digital space for decades. The new AI Act is the latest addition to this complex regulatory landscape.



In 1995, the European Union (EU) adopted its first directive on the processing of personal data. It was followed in 2002 by directive 2002/58 governing electronic communications and cookies (the ePrivacy Directive). 2018 was a landmark year with the entry into application of the General Data Protection Regulation (GDPR) (replacing the Data Protection Directive) which set a new regulatory standard across the world on the processing of personal data with strict rules and hefty fines.

The EU then decided to further regulate online services with the adoption of the Digital Markets Act, the Digital Services Act, the Data Act and the Data Governance Act. The latest (but certainly not last) piece in the regulatory puzzle is the AI Act, which entered into force in summer 2024, and which imposes strict requirements for certain uses of AI. All these laws have an extraterritorial reach and impact US organizations doing business in the EU.

How to Use This Chapter

This chapter seeks to help you navigate the complex EU regulatory framework as you integrate third-party AI tools in your business.

→ Begin with the EU AI Act

1. **Company Role:** Determine your designated role under the AI Act for each AI tool used, whether as a provider or a deployer. This foundational step is crucial for understanding your specific obligations based on the regulatory requirements of the AI tool's designation.
2. **AI Tool Designation:** Identify if any AI tools are classified as AI Systems or GPAI models under the AI Act, and determine their respective risk categories. Based on whether a company is a deployer or a provider, there will be specific regulatory requirements that apply to each AI tool.
3. **Obligations and Compliance:** Based on your role and the AI tool's categorization, outline your obligations under the AI Act. This section underscores the importance of consulting with external counsel to ensure accurate interpretation.
4. **Governance and Risk Management:** Integrate these obligations into a governance program and operationalize them within a risk management framework. Pay special attention to changes in vendor management, legal contracting terms, transparency requirements, and monitoring and reporting processes.

→ Revisit Your Privacy Program

1. **GDPR:** Understand the impact of using AI tools on your existing privacy program, including:
   - needing data protection impact assessments (DPIAs) if your practices include high risks to the rights and freedoms of individuals,
   - updates to data processing agreements (DPAs), confirming controller/processor designations and deciding the legal basis for processing,
   - handling data subject rights and
   - practices around data management (training data, data minimization and security).
2. **ePrivacy Directive Compliance:** While the ePrivacy Directive does not explicitly mention AI, its principles of confidentiality, data protection, and user consent may apply to AI tools that process electronic communications data, use tracking technologies, or engage in direct marketing activities.

→ Confirm Obligations, If Any, in Other Non-AI Legislation

1. **DSA Compliance:** For online companies to which the DSA applies, understand how the DSA impacts the use of AI tools, particularly in content curation and moderation.

The EU AI Act

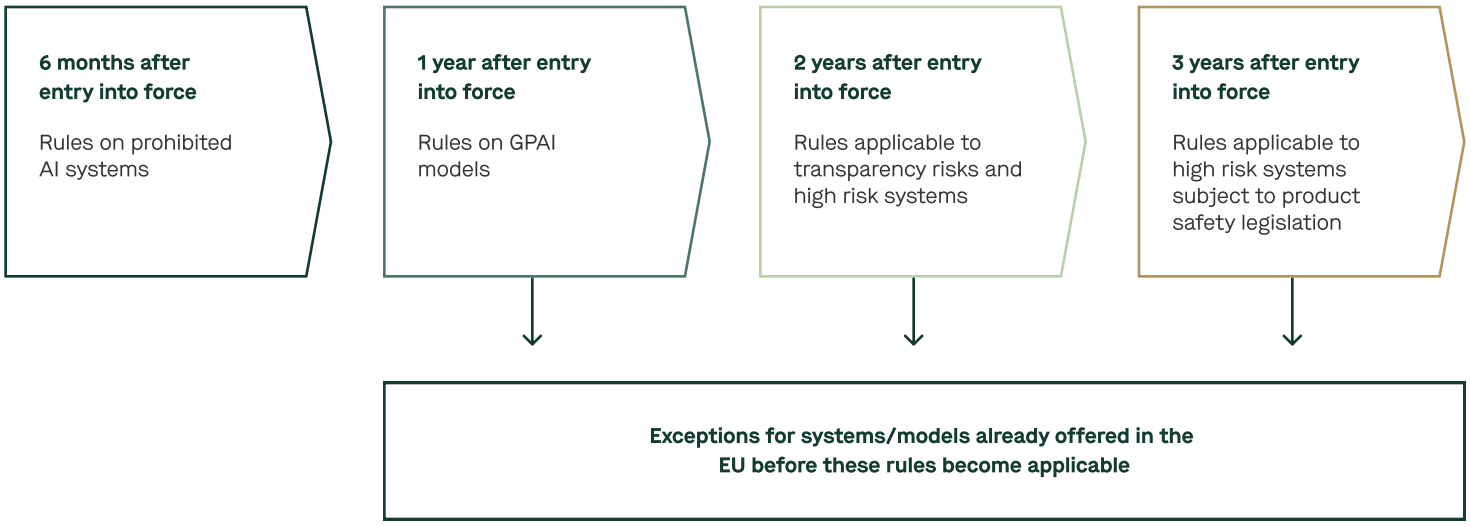
The Framework

What Is the AI Act?

The AI Act introduces a new risk-based legal framework for AI tools that will apply across all industry sectors. The AI Act is not the sequel to the GDPR; it is first and foremost a product safety legislation which integrates safeguards for the protection of fundamental rights of individuals in relation to AI.

When Will It Start to Apply?

The AI Act entered into force in August 2024, and will start to apply in phases as of February 2, 2025. Here is an overview of the key dates:



When Should Companies Get Started with Their Compliance Plan?

- You should identify your company's use of AI tools and assess which AI Act obligations apply to you no later than Q4 2024, at a minimum (*see Chapter Three AI Tool Use Cases and the Range of Risks*). This exercise is necessary in order to be in a position to integrate AI Act compliance into your AI governance framework in the course of 2025, in particular the ban on certain AI systems which will apply as of February 2, 2025.
- If you are considered a "provider" or "deployer" of a "high-risk AI system" tool that is already in the EU market as of the enforcement date, you will only need to comply with the AI Act in the event of a significant change in the "high-risk AI system" tool's design or intended purposes (unless the high-risk AI system is intended to be used by public authorities, in which case compliance is required by August 2, 2030). This means that in limited cases, high-risk AI system tools will not be in scope of the enforcement regime. While this may seem surprising, the requirements for high-risk AI systems are mainly product safety requirements that need to be fulfilled before placing an AI tool on the EU market (e.g., declaration of conformity and applying a CE mark) which would be difficult to apply retrospectively.
- If you are considered a "provider" of a "GPAI" tool and you are already providing it in the EU market as of the enforcement date, you're granted a grace period of two additional years to comply (i.e., providers of GPAI models placed on the market before August 2025 will need to comply by August 2027).

What AI Technologies Does the AI Act Apply To?

The AI Act covers "AI systems" and GPAI models.

→ AI Systems

AI systems have some degree of autonomy and have the capability to "infer." This means that they can derive models and algorithms from inputs and outputs of data, and they can generate outputs including predictions, content, or decisions which can influence physical and virtual environments. Some of these systems are considered "high risk" and others have specific transparency risks. At the time of writing, examples can include:

- a chatbot used by a bank to assist customers with basic queries and transactions. This system uses natural language processing models to understand user inputs and provide relevant responses.
- a computer vision system used in a factory to detect defects on assembly lines. This uses machine-learning models trained on images of defective and non-defective products.
- a recommendation engine used by an e-commerce platform to suggest products to customers based on their browsing and purchase history.

For purposes of this chapter, when we refer to AI systems, we refer to AI tools that qualify as AI systems under the AI Act.

→ GPAI Models

GPAI models are AI models capable of performing a wide range of tasks and that can be integrated in other systems or applications; generally, a GPAI model will usually be integrated into an AI system even though they are both subject to distinct obligations under the AI Act. While GPAI models are essential components of AI systems, they do not constitute AI systems on their own (to become an AI system, an GPAI model requires the addition of other components, like a user interface). GPAI models are usually trained with a large amount of data using self-supervision at scale. GPAI models can be marketed in various ways, including through libraries, APIs, or as direct downloads. As of the date of this writing, examples can include:

- large language models that can generate human-like text across a wide range of topics and tasks, from creative writing to code generation;
- multimodal models that can generate images from text descriptions; and
- speech recognition models that can transcribe audio in multiple languages.

Some GPAI models are considered as **"GPAI models with systemic risk,"** which includes risks that can be propagated at scale across the value chain and that could have a significant impact on the market due to their reach, or negative effects on public health, safety, public security, fundamental rights, or the society as a whole. GPAI models are presumed to pose systemic risks if the amount of computation used for training exceeds 10^25 floating point operations (FLOP). The key distinction is that GPAI models with systemic risk are exceptionally large and powerful models that could potentially have far-reaching impacts due to their scale and generality. The European Commission (EC) has not yet designated any GPAI models as GPAI models with systemic risk.

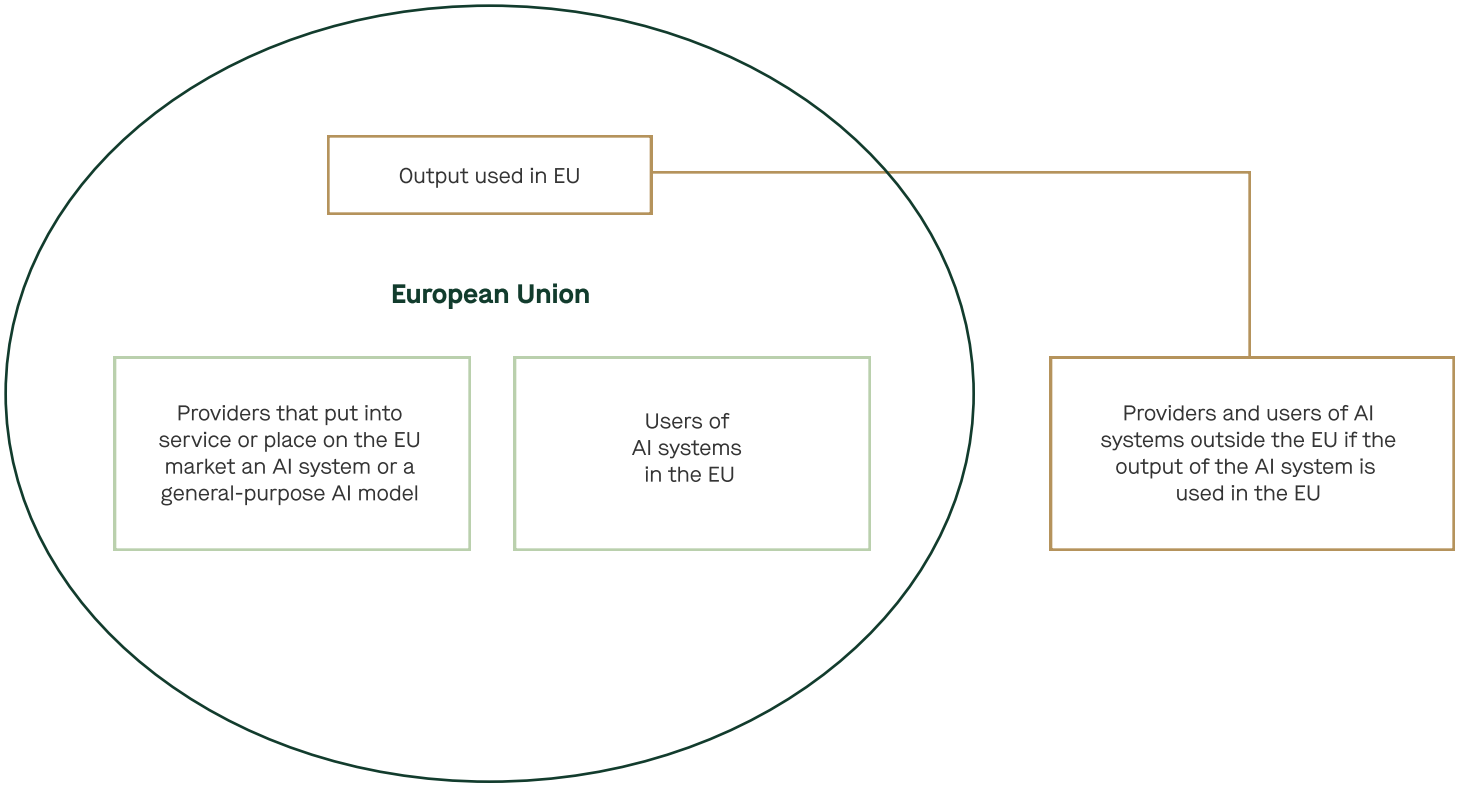
For purposes of this chapter, when we refer to GPAI models, we refer to AI tools that qualify as GPAI models under the AI Act.

The Framework

Who Does the AI Act Apply To?

The AI Act can apply both to companies established inside and outside the EU, including U.S. companies incorporating AI tools into their company operations that sell products in the EU. For instance, the AI Act will apply to:

- companies using AI systems in the EU;
- companies inside or outside the EU which put into service or place on the EU market an AI system or general-purpose AI model. Any kind of selling of an AI system or general-purpose AI model in the EU will fall in this category; and
- companies outside the EU providing or using AI systems where the output of the system is intended to be used in the EU. This notably is to avoid companies circumventing the application of the AI Act where the output of a system provided by a non-EU company would be used by a company in the EU.



EU AI Act Roles and Responsibilities

AI Act Roles

A company will be designated as a **provider, a user/deployer, a distributor, or an importer depending on their activities in the supply chain.** This chapter focuses on **"providers"** and **"deployers."** Since **distributors** are essentially resellers and **importers** are EU companies placing an AI system from a third country on the EU market, they are not included for purposes of this chapter.

In each case, a role will have different obligations under the AI Act based on the designation of a respective AI tool as an AI system vs a GPAI, and the AI tool's corresponding risk categorization.

Providers

Companies that develop (or have a third-party develop), put on the market or into service under their own name or trademark an AI system or general-purpose AI model, whether for payment or free of charge.

Providers bear primary responsibility for compliance with the AI Act.

Deployers

Companies using AI systems or general-purpose AI models.

Deployers have specific obligations under the AI Act, especially when they deploy these systems and models in high-risk contexts.

"Deployers" do not include users using AI in the context of a personal non-professional activity.

Roles and Responsibilities

→ Is Your Role a Provider or a Deployer, or Both?

- The scope of the "deployer" definition is very broad – you will qualify as a deployer when your company uses an AI system, for internal or external purposes. However, simply qualifying as a deployer doesn't mean you have obligations; for example, using an AI tool to schedule appointments is unlikely to trigger any requirements for a deployer (other than the general obligation to ensure AI literacy of users of AI systems (e.g., staff)).
- Other than the general AI literacy obligation, deployers only have obligations under the AI Act in limited circumstances; companies will only need to comply with certain obligations when using AI systems that are classified as (i) high-risk e.g., AI systems that are used by HR for recruiting, or (ii) as having a specific transparency risk under the AI Act (for example, when using an AI system for emotion recognition or biometric categorization).
- Even if you are a deployer under the Act, you may be concurrently designated as a provider depending on your use of the AI tool, with obligations as a deployer and a provider:
  - Most notably, if you incorporate AI tools into your company's operations, you may be a "deployer," but you can become a "provider" when you integrate the AI system into your own products or services.
  - Putting your own trademark on a third-party high-risk AI system will result in having to comply with "provider" obligations under the AI Act.
  - If you are a deployer and you substantially modify a high-risk AI system already on the market or modify an AI system already on the market in a way in which it becomes a high-risk AI system, you will have to comply with "provider" obligations under the AI Act.

Use Cases	Description	Role
Internally Facing	Third-party AI tool used for internal business purposes to enhance employee productivity, often using confidential information but not sensitive information	The company will likely qualify as a deployer. If the AI system is not high-risk and does not raise transparency risks, the deployer will not have obligations under the AI Act (other than the general AI literacy obligation).
Internally Facing	Third-party AI tools used for internal business use to improve workflows using sensitive information or personal data	This application could qualify as high-risk in which case the company as the deployer would be subject to certain obligations under the AI Act.
Externally Facing	Third-party AI tools embedded in workflows building products or services, behind the scenes, e.g., code-generation support	Depending on how the AI system is used, and the level of integration into the product, the company could qualify as a provider or deployer of the AI system. This assessment would involve a case-by-case assessment based on the facts.
Externally Facing	Third-party AI tools embedded in products or services, facing customers, or the general public	Same as above. Depending on how the AI system is used and the level of integration into the product, the company could qualify as a provider or deployer of the AI system. This assessment would involve a case-by-case assessment based on the facts. In some instances, using AI systems directly in customer-facing activities (e.g., user-facing chatbots) will trigger transparency obligations.

Real World Scenario: Deployer or Provider?

A video game publisher GameX has procured a generative AI tool which allows it to create new game characters.

This tool is used only internally, but GameX is considering making it a feature of its games allowing its customers to create their own game characters and interact with them. GameX may be a "deployer" when using the tool internally, but it becomes a provider when this tool becomes part of its products offered to customers.

AI Act in Practice

Because of the respective obligations of different roles under the AI Act, companies acting as providers or as deployers should consider taking the following steps when incorporating an AI tool into their company operations.

The Applicable Regime for the AI Tool

→ AI Systems

The AI Act categorizes AI systems and GPAI models based on risk levels, from minimal risk to unacceptable risk, imposing different obligations on providers or deployers for each category. It also sets standards for transparency, accountability, and data governance, particularly for high-risk AI systems.

The Applicable Regime

You should determine if your company is using an AI tool that fits into one of the following categories of AI Systems:

AI System Categorization	Considerations
Prohibited AI systems: Some AI systems are completely prohibited under the AI Act. These include e.g., AI systems used for the purpose of social scoring or emotions recognition in the workplace (other than for medical or safety reasons).	Do not roll out in the EU.
High-Risk AI systems: The AI Act provides a list of high-risk AI systems. They include e.g., AI systems intended to be used to influence the outcome of an election or the voting behavior of individuals, as safety components in the management and operation of critical infrastructure (for example, digital infrastructure and road traffic), use by law enforcement or for recruitment decisions (e.g., placing job ads or filtering job applications). High-risk AI systems also include any AI system that is a "safety component" of a regulated product or that is itself a regulated product (i.e., products which are required to comply with certain safety standards before being introduced on the EU market e.g., cars, toys). A safety component is a component which fulfills a safety function for a product or AI system, or whose failure or malfunctioning can endanger the health and safety of persons or property.	**Significant obligations apply to providers of high-risk AI systems, including setting-up a quality management system** (mainly consisting of procedures for quality controls, testing, data management, risk management, and post-market monitoring), carrying out a conformity assessment, registering the system with the dedicated public EU database and, for non-EU companies, appointing a representative in the EU. **Some obligations also apply to deployers of high-risk AI systems,** including complying with the providers' instructions, only using relevant and sufficiently representative data, monitoring the functioning of the AI system, and notifying the provider in case of a serious incident.
AI systems with transparency risks: these include AI systems which interact directly with individuals, which 1. can create content or 2. can create deep fakes or 3. are used for emotions recognition or biometric categorization. Subject to certain exceptions, these AI systems include: · systems that interact directly with individuals like chatbots. · systems that create audio, image, video or text content. · systems involving emotion recognition or biometric categorization. · systems creating deep fakes.	Deployers and providers of these types of AI systems have specific transparency obligations. A company procuring such a system should make sure the provider provides sufficient information in order for the company to be able to comply with its transparency obligations.
Minimal risk AI systems: AI systems with limited risks that do not fit in the categories listed above are not subject to obligations pursuant to the AI Act, other than the general obligation for providers and deployers of any AI system to ensure those using AI systems (e.g., staff) have a sufficient level of AI literacy.	The AI Act does not impose obligations (other than ensuring AI literacy), but other risks may need to be addressed, including data protection and intellectual property risks.

The Applicable Regime

→ GPAI Models

When a company procures a GPAI model, its goal will often be to integrate (or "plug it") into its own products or services. For example, a company may procure a large language model to ensure the company's chatbot will be able to process the users' queries. The company selling the chatbot would then act as a provider of an AI system. However, the company would not qualify as a provider of the GPAI model integrated into its chatbot, only the original provider of the GPAI model would.

When you procure a GPAI model, you should determine which category the model fits into and whether the model provider complies with its obligations under the AI Act:

GPAI Model Categorization	Considerations
GPAI Model	Providers of GPAI models have obligations which include e.g., information and documentation requirements, putting in place a policy to comply with copyright law and making publicly available information about the content used for the training of the model.
GPAI Model with Systemic Risks	Providers of GPAI models with systemic risks are subject to a set of additional obligations, including to perform model evaluations, assessing and mitigating risks, keeping track and reporting serious incidents and ensuring an adequate level of cybersecurity protection.

Governance

An AI governance framework is essential to ensure that using AI tools result in positive outcomes for companies and that risks are mitigated.

It is recommended to follow the Provenance/Input/Output Governance Architecture model (PIO) discussed in *Chapter Four, Deployment Stages and Types of Risks* when assessing risk, and to develop a defensible governance program with operational risk management features, such as cross-functional committee oversight, policies, vendor management programs and ongoing monitoring, reporting, and escalation processes responsible for addressing AI risks, as discussed in *Chapter Five, Addressing Risks of Using AI Tools through Corporate Governance*. Organizations that offer products or services in the EU should conduct their risk assessments and identify their legal obligations as a starting point, and then embed the relevant compliance measures in a documented compliance program.

Several key aspects of your governance program will need to be updated for AI Act obligations, most notably:

- → the vendor management program's diligence process,
- → the Legal team's contracting terms,
- → transparency to recipients of AI systems with transparency risks,
- → monitoring and reporting processes,
- → registration of high-risk AI systems by providers, and
- → incident management programs of serious incidents to regulators.

Governance

→ Due Diligence

When procuring AI tools, as part of your vendor management program, you should pay specific attention to the provider's compliance with the AI Act.

Here are some examples of requirements which can be included in due diligence lists:

Examples of General Due Diligence Questions for All AI Tools

- Explain what data set was used to train the AI system / GPAI model.
- Explain how the AI system / GPAI model will continue to be trained (including with what data).
- Explain how input data will be re-used by the provider.
- Explain how bias has been addressed (especially regarding demographic diversity, geographic relevance, and temporal validity).
- Confirm adequate documentation and instructions to use the AI system / GPAI model have been provided.
- Confirm that sufficient information will be provided to comply with transparency requirements.
- Explain the capabilities and limitations of the AI system / GPAI model.
- Explain whether activity logs are generated and how long they are retained.

Examples of Due Diligence Questions Specific to AI Systems with Transparency Risks

- Confirm that AI generated content is labeled as such.

Examples of Due Diligence Questions for High-Risk AI Systems

- Confirm that a quality management system is in place.
- Confirm that quality controls, testing, data management, and risk management processes are implemented.
- Confirm that a conformity assessment has been conducted.
- Describe human oversight measures that are built into the system.
- Provide any fundamental rights assessment conducted.
- Provide contact information to notify serious incidents.
- Provide contact details of an authorized representative in the EU.

Examples of Due Diligence Questions Specific to GPAI Models

- Confirm that a policy respecting EU copyright law has been implemented.
- Confirm that a summary of the AI model training data is publicly available.

Governance

→ Contracting with the Provider

When procuring AI tools, as part of your vendor management program or as a part of the Legal function's responsibilities, pay specific attention to the contract terms negotiated with the provider. Existing contractual clauses in templates may need to be adapted and new clauses added.

For example, the following contractual clause could be integrated into agreements:

- **Compliance with the AI Act:** A commitment that the AI tool complies with the AI Act during the term of the agreement.
- **Authorized uses:** List of authorized uses of the AI tool, including for business purposes.
- **Documentation:** Obligation to document compliance with AI Act and to provide documentation (including risk assessments upon request).
- **Record-keeping:** Commitment that the AI tool has been designed to allow the generation and retention of logs to ensure traceability.
- **Human oversight:** Commitment of the provider to have a process for and implement human oversight. Alternatively, the agreement can also allocate responsibility between the provider and the deployer to carry out human oversight activities.
- **Explainability:** Commitment that clear explanations for all decisions affecting individuals, including key factors taken into account, can be provided by the provider.
- **Data sets:** Commitment that data sets used to develop the AI tool are relevant, representative, free of errors, and be as complete as possible in relation to the purpose of the tool.
- **Security Audits:** audit routines of providers of AI systems.

Whether or not it is useful to add such clauses to agreements should be assessed on a case-by-case basis.

PRO TIPS:
Integrating AI in your own products and services

If a company procures an AI tool to be integrated into a service they provide to customers, the company may itself become the provider of an AI system.

In such a case, the company should make sure that the commitments made to customers are mirrored, as needed, in the agreement with the AI tool provider.

Governance

→ User Transparency

Because AI systems with specific transparency risks are subject to heightened transparency obligations, if you incorporate these AI tools into your operations, you need to inform individuals that they are interacting with an AI system or that the content they are viewing is AI generated, unless it is obvious from the context.

In practice, this audience includes the general public/ prospective customers, existing customers or partners, and if you have offices in EU countries where an employee works council is in place, it may also be necessary to inform and consult the works council when the AI tool used affects employees of a company.

PRO TIPS:
Providing information just in time

Information should be provided in a format adapted to the AI tool concerned.

For example, if a user is interacting with a chatbot through text messaging, the first text message provided by the AI system could mention the service is AI powered.

→ Monitoring and Reporting

Compliance with the obligations under the AI Act continues after your integration of the AI system tool into your operations. Ongoing monitoring of AI systems is a central part of the governance process, as discussed in *Chapter Five, Addressing Risks of Using AI Tools through Corporate Governance*.

Under the AI Act, providers of high-risk AI systems have specific obligations to monitor the functioning of AI tools, including by recording events (i.e., logging capabilities). The goal of this monitoring is to take preventive and corrective action in order to prevent harmful consequences to the use of AI systems.

Deployers have an indirect obligation to monitor high-risk AI systems they use as they have an obligation to report serious incidents to providers, distributors and importers and to authorities in certain cases (*see "Notification of serious incidents" on the next page*).

PRO TIPS:
Monitoring AI systems

Both provider and deployers should implement monitoring measures.

AI systems' performance and outcomes should be regularly monitored for issues or deviations from expected behavior.

AI systems should be integrated into security audit routines.

Record-keeping is essential: logs of AI systems use should be retained.

Governance

→ Transparency to Regulators

- **Registration of High-Risk AI Systems.** High-risk AI systems and providers of such systems (or their representative) will need to be registered with an EU database to be set up by the EC.
- **Notification of serious incidents.** Providers of high-risk AI systems and GPAI models with systemic risks and, in certain cases, deployers, have an obligation to notify competent authorities of incidents or malfunctioning of AI systems which lead to serious consequences. These are called "serious incidents."

- While the notification obligation lies primarily with providers, deployers can also have an obligation to notify these incidents directly with authorities where they are not able to report the incident to the provider.

PRO TIPS:
Have a process to report serious incidents

Companies using AI systems either as providers or deployers should consider whether they are required to have a system for notifying serious incidents.

Providers' process concerns reporting to authorities.

Deployers' process concerns reporting first to providers, then to distributors and importers. The process should also cover notification to authorities where notification of the provider is impossible.

In certain case, suspension of the use of the AI system may be required.

General Data Protection Regulation (GDPR)

The GDPR is not AI-specific, but it applies when an AI system or model processes personal data.

It imposes strict obligations on organizations processing personal data. It has an extraterritorial reach and applies also to organizations established outside of the EU, if they offer their products or services to individuals in the EU or monitor the behavior of individuals in the EU. The GDPR has been implemented into UK law. The same requirements for data processing therefore apply also under UK law.

The GDPR has profound implications for the development of AI systems and models, both in the training and deployment phases. GDPR principles such as data minimization, limitation of retention periods and data subject rights affect the training and deployment of AI systems and models. The GDPR also includes rules that impact certain AI use cases, such as automated decision-making in relation to individuals.

Roles and Responsibilities

Under the GDPR, an organization is typically a controller for the personal data that it processes as part of a B2C offering. However, an organization may qualify both as a controller and as a processor when offering a B2B product e.g. a vendor processing personal data on behalf of a business customer (processor) and reusing the data to improve its product (controller).

The main obligations of the GDPR apply only to controllers, such as providing a privacy notice, ensuring a legal ground for data processing, and handling individuals' requests to exercise their rights to their data. Processors have specific obligations, including to ensure they implement adequate security measures and report data breaches to controllers. When a controller integrates a third-party's AI tool into its products or services, it will need to identify the role of the vendor i.e., controller or processor, and ensure that the contract with the third party provider appropriately reflects this role.

Typically, the AI tool vendor will be a processor for the personal data that it processes on the customer's behalf (e.g., end user data), but a controller for its own data processing to train its AI models. You should carefully assess the use that the AI tool intends to make of your personal data and whether or not to permit re-use of the data to train the vendor's AI model. Once this is decided, you should establish your respective roles and responsibilities in a data processing agreement.

Real World Scenario: Controller or Processor?

A video game publisher GameX has procured a generative AI tool which allows it to create characters that can chat with players.

GameX is a "controller" for the personal data of players that it processes to provide its services, including data that players share with virtual characters.

The third party AI provider processes such data as a "processor" on behalf of GameX, but may qualify as a "controller" if it re-uses the data to train its AI model.

GDPR in Practice

This section gives an overview of the GDPR requirements that apply when integrating a third party AI tool in products or services.

The Applicable Regime for You and for the AI Tool

Roles and responsibilities under the AI Act and the GDPR are different and apply concurrently. While the AI Act classifies organizations based on their role as providers, importers, distributors, and/or deployers of AI tools, the GDPR classifies them as either controllers (i.e., they determine the purposes and means of the processing) or processors (i.e., they process data on behalf of a data controller). Obligations under the GDPR will flow from an organization's role as controller or provider.

The strictest obligations of the GDPR apply to the most intrusive/risky types of data processing. For instance, the use of sensitive personal data (e.g., health data) is very restricted and typically requires individuals' explicit consent. Also, when you carry out processing activities that entail a high risk for individuals, you will need to carry out a data protection impact assessment (in addition to any risk assessments carried out under the AI Act).

When AI is used in products or services offered to children, you should carefully consider regulatory guidance on age appropriate design, such as the UK Information Commissioner's Office Age Appropriate Design Code.

Real World Scenario: Applicable Regime?

A video game publisher GameX has procured a generative AI tool which allows it to create characters that can chat with underage players.

In addition to complying with standard GDPR requirements (such as providing a privacy notice), GameX will likely need to carry out a data protection impact assessment and implement measures to protect the best interests of underage users (e.g., protecting against harmful content).

Governance

Most companies have established comprehensive privacy programs incorporating DPIA results and corresponding privacy requirements into their policy, vendor management and ongoing monitoring, reporting and escalation activities.

Check several key aspects of your privacy governance program, most notably:

- the vendor management program's diligence process,
- the Legal team's contracting terms,
- data subject information, and
- compliance requirements.

→ Due Diligence

Before procuring an AI system or GPAI model, you should conduct adequate due diligence on the AI tool to ensure that its provider complies with the requirements of the GDPR and that using the tool will not hinder your own GDPR compliance.

This includes knowing how an AI tool has been trained, the source of the data used for training, what safeguards are implemented to prevent bias, how irrelevant data is excluded and what security measures have been implemented.

Examples of Privacy Due Diligence Questions for AI Tools

- Explain whether personal data was used to train the AI system / GPAI model and if so, which steps the provider has taken to ensure GDPR compliance.
- Explain the source of personal data used by the provider.
- Explain security measures that the provider has in place to protect personal data.
- Explain the bases for processing personal data — legitimate interest, consent or other?
- Confirm that the provider implemented safeguards to prevent bias in its AI tool.
- Explain any measures taken to filter out irrelevant or inaccurate data.
- Explain any measures taken to pseudonymize or anonymize personal data.
- Explain how input and output data will be re-used by the provider.

→ Contracting with the Provider

Once an AI tool has been selected, the next step is to enter into a data processing agreement which will address the specific requirements of the GDPR. The agreement should include mandatory clauses set out in Article 28 of the GDPR if the provider acts as a processor on behalf of the customer. If the provider acts as a controller, the data processing agreement should include provisions setting out the roles and responsibilities of parties as controllers. In addition, if the engagement with the vendor involves a data flow outside of the EU, the parties should implement a data transfer mechanism to legitimize the data flows (subject to exceptions). The most common solutions are to include the EC's standard contractual clauses for international data transfers in the data processing agreement or referring to the providers' EU-US (or UK-US) Data Privacy Framework self-certification, where applicable.

→ Data Subject Information

The GDPR requires informing individuals regarding the use of their personal data and documenting compliance.

☐ **Information Notice**

When using a new AI tool, you may need to update the notices you provide to individuals about the processing of their personal data, which is usually in the form of a privacy policy to individuals. The notice should cover the purposes of the AI tool's processing, the categories of personal data involved, the legal basis for the processing, the recipients of the data, information about the logic involved in any automated decision making have legal or similar effects as well as significance and consequences thereof and any transfers of personal data outside the EU.

☐ **Choice of legal basis for processing**

Attention should be given to the choice of the applicable legal basis of the processing. For instance, for AI training purposes, legitimate interests may be the applicable legal basis in some cases, but consent or contract may be appropriate in other cases. Where legitimate interest is the applicable legal basis a "legitimate interest assessment" must be documented. When using data for a purpose other than for which the data was initially collected, the controller should make sure the new purpose is compatible with the purpose for which the data was collected.

If sensitive categories of personal data are also processed (e.g., health data), additional strict requirements will apply. The processing of such categories of personal data should be considered on a case-by-case basis.

☐ **Rights handling procedures**

Using AI tools may require an update to your GDPR rights handling procedure.

Here are some examples of how a GDPR rights handling procedure may need to be updated:

- **Automated decision-making:** When an AI tool is used to make a decision about an individual which has legal or similar effects, it will in certain circumstances be required for a company to allow individuals to have the decision taken by a human or allow them to challenge the decision and obtain human intervention.
- **Right of access:** Where an individual makes an access request in relation to a data processing involving automated decision making, meaningful information about the logic involved, and the significance and consequences of the processing should be provided.
- **Involvement of the AI tool provider:** The AI tool provider may need to be involved in the preparation of responses to data subject requests. Processes should reflect when and how the provider should be reached out to.

GDPR in Practice // Governance

→ Compliance Activities

- [ ] **DPIA where required**

When the processing of personal data with an AI tool can result in high risks for the rights and freedoms of individuals, a data protection impact assessment (DPIA) is required.

The concept of "high risk" under the GDPR is different from the concept of "high risk" under the AI Act. Generally speaking, a high-risk AI system under the AI Act will likely result in high risks for the rights and freedoms of individuals under the GDPR and will require a DPIA. However, using an AI tool which is not "high risk" under the AI Act does not automatically mean no DPIA is required. A DPIA will still be required if the processing of personal data with the AI tool can result in high risks for the rights and freedoms of individuals.

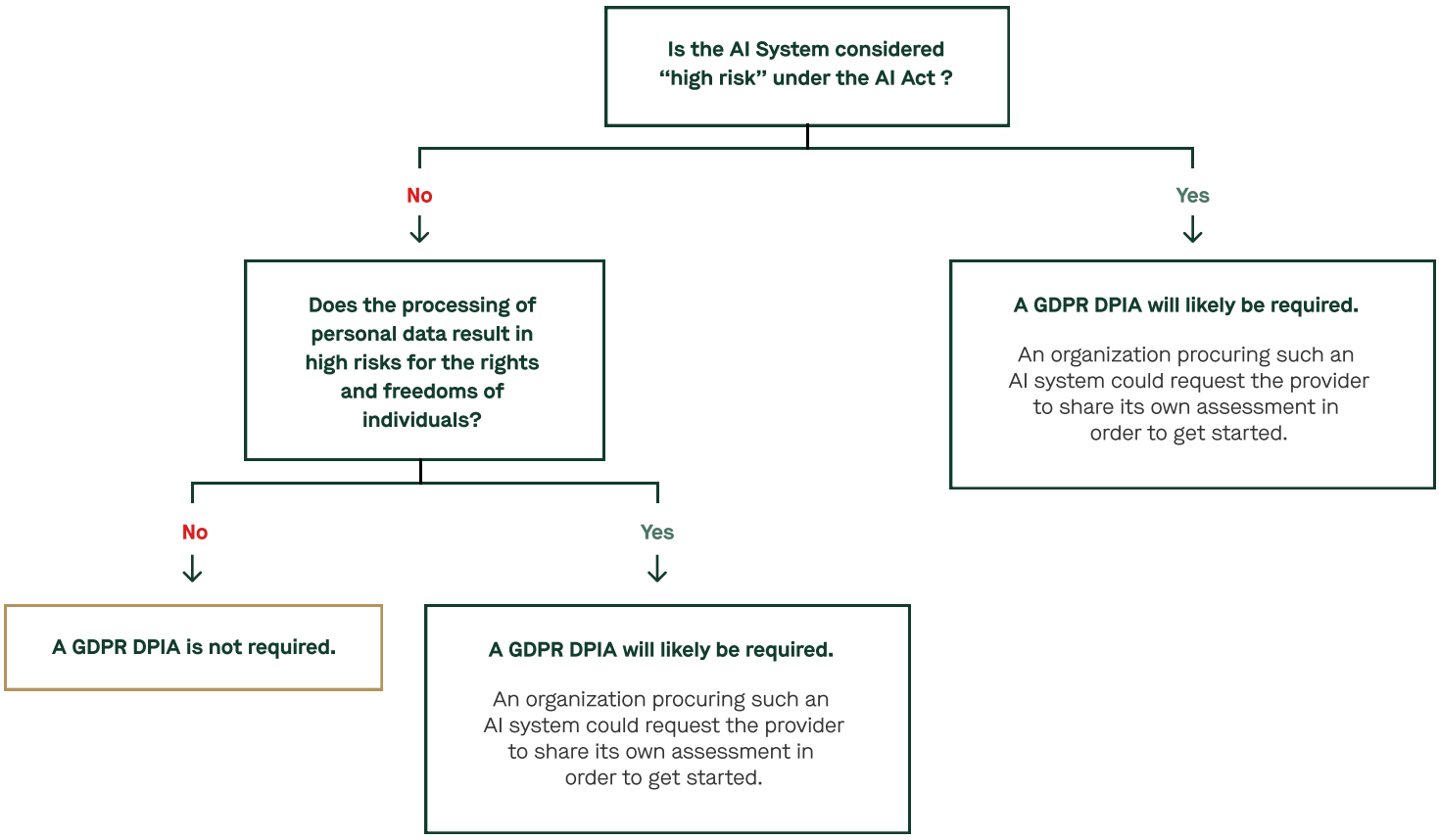
- [ ] **Security policies**

In addition, the GDPR requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. When using an AI tool, this means internal security policies may need to be reviewed to take into account specific risks.

For instance, AI tools usually process a very large amount of data which means that risks, including cybersecurity risks, are increased. Additional measures may therefore be needed to restrict access to data to specific individuals, set deletion rules to avoid keeping data which is not relevant anymore and to pseudonymize or anonymize data, where relevant.

- [ ] **Training**

Teams using AI tools to process personal data should receive specific training in order to allow them to identify when AI is being used (which is not always obvious) and in which cases it is appropriate to process personal data using AI tools.



ePrivacy Directive

The ePrivacy Directive complements the GDPR and specifically addresses privacy in electronic communications. It includes provisions on the confidentiality of communications, which can be pertinent to AI tools in messaging, voice services, and other communication technologies.

Use Case: Using AI to Track Online User Behavior

Online services may use AI to track users' behavior, including to carry out analytics or to provide behavioral advertising.

- **Provide notice and obtain consent:** The ePrivacy Directive requires website providers to obtain users' informed consent to the use of cookies and similar technologies, subject to limited exceptions. Consent should be obtained through granular consent tools that allow users to easily enable and disable these technologies. Users should be able to retrieve the consent tool to change their preferences at any time. Users' choices should be appropriately documented.
- **Determine parties' responsibilities for cookie consent.** Organizations using a third-party tool to track user behavior should contractually stipulate parties' roles with regard to the personal data collected by the tool and determine which party will be responsible for obtaining users' consent.

Digital Services Act (DSA)

What is the DSA?

The DSA, which became fully applicable on February 17, 2024, imposes strict new obligations in relation to online services offered in the EU such as intermediary services (internet access providers, domain name registrars, VPNs, caching services (CDNs and reverse proxies), cloud and web hosting services, social media networks, marketplaces, app stores, content sharing platforms, online platforms, and Very Large Online Platforms or Search Engines.

Application to AI Tools

The DSA impacts how these companies, especially those considered as online platforms or search engines, use AI tools.

All organizations that are in scope of the DSA need to comply with new requirements relating to the handling of user content, including detailing content moderation rules in their T&Cs, and publishing yearly reports on their content moderation activities. Hosting providers need to also implement a notice and action mechanism to act against illegal content and provide users with a statement of reasons if their content or account is removed or restricted.

Additional obligations apply to online platforms. For instance, they need to refrain from using “dark patterns” that impair users’ ability to make autonomous decisions. They also need to be transparent about their online advertising and any “recommender systems” they put in place (i.e., any system for determining which content is presented to which users).

Very large online platforms and very large online search engines will also need to provide users with the option to not have content recommendations that are based on profiling. Such large organizations are also subject to other requirements, such as the obligation to assess and mitigate systemic risks related to their services. This includes assessing any risks related to the use of AI (e.g., the risk of wide scale propagation of disinformation through AI-powered recommender systems). The measures taken to mitigate systemic risks need to be reported to the competent regulators upon request.

Application to AI Tools

Below are two AI use cases that trigger obligations under the DSA:

Use Case 1: Using AI for Content Moderation

In-scope organizations need to ensure their content moderation activities comply with the DSA's requirements.

- **Content of T&Cs:** T&Cs will need to explain the processes for algorithmic decision-making.
- **Information about content moderation:** At least once a year, organizations will need to publish information about the content moderation they engaged in. Such transparency reports need to contain information about the use of automated tools, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated tools, and any safeguards applied.
- **Explaining decisions:** When organizations take a content moderation decision, they need to explain their decision to the affected user, including where applicable, information on the use made of automated means in taking the decision.
- **Documentation:** Organizations using AI for content moderation will need to document the functioning of the AI and keep such documentation on file. Regulators may require very large online platforms and search engines to provide information demonstrating their DSA compliance, including data on the functioning and testing of their algorithmic systems for content moderation
- **Requirements applicable to providers:** Organizations that rely on third-party AI tools for their content moderation processes will need to ensure they receive sufficiently detailed information to be able to comply with these obligations. This includes AI tools that are merely used to automate the intake process for DSA notices.

Use Case 2: Using AI to Determine How Content Is Presented

Online platforms may use AI to curate how content is presented to users e.g., which video is shown next on a video sharing platform.

- **Explaining recommender systems:** The DSA requires online platforms to explain to users, in an intelligible manner, how their recommender systems work. In particular, online platforms need to explain the key criteria in determining which information is suggested to users and why the information is prioritized for them. To be able to comply with this requirement, online platforms relying on technology offered by third parties should ensure they receive sufficient information from such third parties.
- **User control over recommender systems:** Online platforms need to offer users the ability to control the recommender system. Very large online platforms and search engines will need to offer at least one recommender system that is not based on profiling (e.g., through extensive tracking of users' online behavior). Online platforms should ensure that any third-party technology they use has these capabilities.
- **Avoiding dark patterns:** Online platforms should, in any event, refrain from using AI to manipulate a user's decision-making e.g., by repeatedly presenting pop-ups requesting the user to make a choice where that choice has already been made.

UK Online Safety Act (OSA)

What Is the OSA?

The UK Online Safety Act 2023 (OSA), which was enacted in October 2023, creates a new legal framework for online services, in particular user-to-user services and search services. It is often referred to as the UK's answer to the EU's DSA. However, there are distinct differences between both pieces of legislation. In particular, the OSA focuses on online safety risks and requires all in-scope services to carry out and document risk assessments, whereas the DSA only requires the largest platforms to carry out such assessments, and also deals with other topics such as online profiling.

Using AI to Detect Harmful Content

The UK's online safety regulator "Ofcom" will issue guidance and codes of practice on the measures that companies need to put in place to comply with their online safety obligations under the OSA. The duties under the OSA will become applicable as this guidance becomes available. This phased approach is set out in Ofcom's Roadmap to Regulation, which provides a timeline for the OSA's application.

The first provisions to apply (towards the end of 2024) are the illegal content safety duties, which require in-scope service providers to assess the likelihood of specific types of illegal content being available on their service, or their service being used to commit certain offenses. Service providers will need to implement measures (which may include AI tools) to mitigate those risks.

The OSA gives Ofcom the power to require in-scope providers to use specific Ofcom-accredited technology to detect terrorism content or child abuse content. On this basis, Ofcom will determine the minimum standards of accuracy in the detection of such content that technology must meet in order to be accredited by Ofcom. These standards are expected to be issued in 2025. In-scope providers are advised to monitor these developments closely.

If you have any questions on this Chapter or other parts of the Playbook, or if you'd like an introduction to the sponsors who wrote this Chapter, please use this form.

Use Case: AI Tools to Mitigate Risks

In-scope organizations need to assess new risk mitigation obligations under the OSA.

- **Assess likelihood of illegal content on the service:** Carry out an assessment to determine the likelihood of specific types of illegal content being available on the service, or the service being used to commit certain offenses.
- **Mitigate risks:** Implement measures to mitigate the risk related to illegal content being available on the service, or the service being used to commit certain offenses. Organizations may be required to use Ofcom-accredited technology.