Author

Alessandro Rossi
arossi@explegal.it
+39 02 305 73 57 3

Focus Team Data Protection & Privacy

Using artificial intelligence in business: a practical guide to the EU AI Act

November 11, 2026

For a company introducing artificial intelligence into its operations, the legal assessment should start with how the technology will be used, who will use it and which decisions or activities it will support.

The EU Artificial Intelligence Act, Regulation (EU) 2024/1689, regulates both providers of AI systems and businesses using them. Purchasing a solution from a third party therefore does not, in itself, remove the need to assess the company's own obligations.

For businesses operating in Italy and across the European Union, that assessment should be coordinated with supplier contracts, data protection, employment rules and the management of liability risks.

1. Identifying AI systems and the role of the business

A useful first step is to identify the AI systems used within the organisation, including tools adopted directly by individual departments or employees. Relevant applications may include drafting assistants, customer service chatbots, recruitment software and systems generating marketing materials.

Under Article 3, a business using an AI system under its authority will generally qualify as a deployer. A company developing, or commissioning the development of, a system and placing it on the market or putting it into service under its own name may instead qualify as a provider, including in certain cases involving internal use.

The role should also be reassessed when a system is modified or integrated into a new service. Article 25 identifies specific circumstances in which an operator assumes provider obligations for a high-risk system. These include placing its name or trademark on an existing high-risk system, making a substantial modification that leaves the system classified as high-risk, or changing the intended purpose of a previously non-high-risk system so that it becomes high-risk.

For international groups, the territorial scope also matters. Article 2 can cover providers and deployers established outside the EU where the output produced by the system is used in the Union.

This document is for general informational purposes only and does not constitute legal advice or create an attorney-client relationship.

2. Assessing the intended use and the applicable requirements

The AI Act does not impose the same requirements on every application. A business should first determine whether the proposed use involves a prohibited practice, falls within the high-risk framework or triggers specific transparency obligations. Specific transparency obligations may apply alongside the requirements for high-risk systems.

Certain recruitment and employee management applications are listed in Annex III. These include systems intended to filter job applications, evaluate candidates or make decisions concerning promotion or termination. The exceptions under Article 6(3) require a specific assessment of the system's function and its influence on decisions. The presence of a human reviewer does not automatically exclude high-risk classification. An Annex III system that profiles natural persons remains high-risk.

The insurance example is equally specific: Annex III covers AI systems intended for risk assessment and pricing in relation to natural persons in life and health insurance. This category should not be extended automatically to all insurance activities.

For other applications, such as a tool preparing an initial draft of a commercial presentation, high-risk classification should not be presumed. Its intended purpose and functionality still require assessment, together with any relevant transparency rules and obligations under other legislation.

3. Understanding which obligations apply and when

The implementation timetable must be read in light of Regulation (EU) 2026/1744, the AI Omnibus, which entered into force on 27 July 2026 and amended the original AI Act.

AI literacy requirements and the original prohibited practices have applied since 2 February 2025. Article 50 transparency obligations have applied since 2 August 2026. The main requirements and obligations in Chapter III, Sections 1 to 3, apply from 2 December 2027 to high-risk systems under Annex III and from 2 August 2028 to those classified under Article 6(1) and Annex I, subject to the applicable exceptions and transitional provisions.

Providers of AI systems generating synthetic content that were placed on the market before 2 August 2026 have until 2 December 2026 to comply with the marking and detection obligations under Article 50(2). This does not postpone deployers' disclosure obligations.

Businesses should therefore distinguish obligations already applicable from those requiring preparation for a later date. Existing privacy, employment and contractual obligations remain relevant throughout.

4. Establishing internal rules and supporting AI literacy

Article 4, as amended, requires providers and deployers to take measures supporting the development of AI literacy among staff and other persons operating or using systems on their behalf. Those measures should reflect their knowledge and experience, the context of use and the people affected. The provision does not require a guaranteed level of literacy for each individual.

Practical measures may include guidance on the limitations of the tools used, training for relevant roles and instructions on when an output requires verification. An employee using AI to draft correspondence will need different guidance from a team using it to support recruitment decisions.

An internal policy can help identify authorized tools, restrict the information entered into them and assign responsibility for reviewing outputs. It can also establish a procedure for reporting errors or inappropriate uses.

These organizational measures should be proportionate to the company's activities and may be organized within existing business functions, provided the applicable obligations are met.

5. Reviewing contracts with AI suppliers

The supplier contract should reflect the way the business intends to use the system. General statements that a solution is compliant with the AI Act are of limited practical value unless the relevant role, intended purpose and supporting documentation are clear.

Before adopting a tool, businesses should review the permitted uses, any restrictions on integration or modification, and the supplier's commitments concerning documentation, support and changes to the service. Where relevant, the contract should address cooperation in investigating incidents and obtaining information needed to meet regulatory obligations.

Particular attention should be paid to whether prompts, uploaded documents or other customer data may be retained or used for training, and whether contractual settings allow that use to be restricted.

Liability provisions also deserve review. Limitations of liability, exclusions and indemnities determine how certain losses are allocated between the parties, subject to applicable law. They should be assessed against the consequences of the intended use. Contractual allocation does not, by itself, remove the statutory obligations applicable to the business.

6. Protecting personal data and business information

Uploading a document to an AI tool may involve personal data, confidential commercial information or material protected by third-party rights. Each category requires a separate assessment.

Where personal data are processed, the GDPR continues to apply. Businesses must assess their role and the applicable data protection obligations. Where acting as controllers, they must establish a lawful basis and provide the required information to individuals. Depending on the arrangement, they should also assess the supplier's role, the applicable processing terms and any transfers outside the European Economic Area. Where the conditions set out in Article 35 GDPR are met, the controller must carry out a data protection impact assessment before the processing begins. Businesses should also assess Article 22 GDPR where AI is used for decisions based solely on automated processing that produce legal or similarly significant effects on individuals.

For confidential information, the practical questions include who may access it, how long it is retained and whether it can be reused. Employees should receive clear instructions before uploading customer files, internal reports or commercially sensitive documents.

Intellectual property should also be addressed through the supplier's terms and the intended use of outputs. A contractual permission to use generated material should not be treated as a guarantee that it is free from third-party rights. Review is particularly advisable before using outputs in public campaigns or incorporating them into products and services.

7. Managing transparency in customer interactions and published content

Article 50 distinguishes between obligations imposed on providers and those imposed on deployers. This distinction matters when a business introduces a chatbot or publishes content created with AI.

For systems intended to interact directly with individuals, Article 50(1) requires providers to ensure that people are informed that they are interacting with AI, unless this is obvious in the circumstances. A business deploying a chatbot should verify how the information will be presented and whether its own development or integration activities also make it a provider.

A deepfake is AI-generated or AI-manipulated image, audio or video content that imitates existing persons, objects, places, entities or events and falsely appears genuine. Deployers must disclose when image, audio or video content constitutes a deepfake, subject to statutory exceptions and tailored disclosure rules for evidently artistic or fictional works. They must also disclose AI-generated or manipulated text published to inform the public on matters of public interest, subject to the statutory exceptions. For such texts, an exception applies where there is substantive human review or editorial control and a person or legal entity holds editorial responsibility for publication.

These rules do not establish a general obligation for a deployer to add a disclaimer to every AI-assisted marketing text or image. The specific content and publication context must be assessed. Standard editing, synthetic content and deepfakes should not be treated as interchangeable concepts. The European Commission's transparency guidelines provide further clarification.

Where disclosure is required, the information must be clear and distinguishable and provided by the first interaction or exposure. Consumer protection, advertising and privacy rules may impose additional requirements.

8. Assessing liability and insurance coverage

An AI output may contain inaccurate information, lead to an unsuitable recommendation or reproduce protected material. Businesses should assess the consequences of those errors before relying on a system for decisions affecting customers, employees or third parties.

A proportionate review process can help reduce the likelihood of harm and document how the business used the system. For high-risk applications, the applicable framework also includes specific requirements concerning competent human oversight and monitoring, to be implemented according to the relevant timetable. Article 26 sets out the relevant deployer obligations.

The allocation of civil liability depends on the facts, the applicable law and the parties' contractual arrangements. Regulatory compliance alone does not resolve every question concerning compensation for harm.

Businesses should also review whether existing cyber, professional liability or product liability policies respond to the risks associated with their intended AI use. Coverage depends on the policy wording, exclusions and applicable law. Where the proposed use changes the insured activities or risk profile, the position should be discussed with the insurer or intermediary before assuming that existing cover is sufficient.

9. Planning adoption before expanding AI use

A practical adoption plan should connect the legal assessment to the people responsible for procurement, technology, human resources and the relevant business activity.

Before expanding a pilot project, the company should confirm the intended use, its regulatory role and the applicable requirements; review the supplier terms and data flows; and put in place appropriate instructions and oversight. The assessment should be revisited when the purpose, functionality or supplier arrangements change.

This approach helps businesses identify the obligations relevant to their operations and address contractual and organizational issues before AI becomes embedded in services or decision-making processes.

***

EXP Legal assists businesses and international groups in assessing the legal implications of adopting artificial intelligence, reviewing supplier and customer contracts, preparing internal policies and coordinating AI Act requirements with data protection, employment and liability considerations. Our insurance law practice also supports the assessment of relevant coverage and contractual risk allocation.

This document is for general informational purposes only and does not constitute legal advice or create an attorney-client relationship.