The EU AI Act: how does it apply to you?

OMB | Large Corporate | International Tax

October 2026

22 September 2026

We consider when a UK tax practice could fall within the EU's AI rules and set out eight practical steps to manage the risks.

Key Points

What is the issue?

The EU AI Act can apply to UK tax practices when AI-generated outputs are used in the EU. Different obligations apply according to the system's purpose and risk, with substantial penalties for non-compliance.

What does it mean to me?

Firms must determine which AI systems they deploy, where their outputs are used and whether any use is high-risk. Existing professional responsibilities for accuracy,

confidentiality, transparency and human oversight continue to apply.

What can I take away?
Maintain an AI systems register, investigate EU connections, classify each use and keep qualified people in control. Protect client information, check suppliers, explain significant AI use, train staff and prepare for incidents.

Artificial intelligence is becoming part of everyday professional practice. Tax advisers may use it to research legislation, summarise documents, draft correspondence, take meeting notes or support calculations. Firms may also encounter AI in recruitment, client onboarding and other business processes.

Many UK firms nevertheless assume that the European Union's rules on AI do not concern them. After all, they are established outside the EU and may provide principally, or even exclusively, UK tax advice. That assumption needs to be tested.

Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the EU AI Act) can apply to providers and deployers established outside the EU where output produced by an AI system is used in the EU. For a UK tax practice, the potential connection might arise where AI-assisted work is supplied to an EU-based client or used by an office, group company or other party in the EU.

The Act is complex and its provisions are being introduced in stages. Not every use of AI will be regulated in the same way and an EU connection does not automatically make a system high-risk. The practical task is to identify the firm's AI systems, understand where their outputs are used and apply controls proportionate to the particular use.

What is the EU AI Act?

The EU AI Act creates a common legal framework for AI across the EU. It seeks to support innovation and the EU internal market while protecting health, safety and fundamental rights. The EU AI Act takes a risk-based approach, with the applicable rules depending on the nature, purpose and potential effects of the system. See ***Understanding the risk categories***.

Most tax practices using an externally supplied AI tool without substantially changing it are likely to be ‘deployers’. In broad terms, a deployer is a person or organisation using an AI system under its authority, other than for a purely personal, non-professional activity.

A firm that develops a system, markets it under its own name or makes a substantial modification may instead acquire the more demanding responsibilities of a provider and should take specialist advice.

The timing also matters. The Act entered into force on 1 August 2024, with its provisions taking effect in stages. Following the July 2026 AI Omnibus, the rules for high-risk systems listed in Annex III, including certain employment and recruitment systems, are due to apply from 2 December 2027. Rules for high-risk systems embedded in regulated products are due to apply from 2 August 2028. Some provisions, including prohibitions and transparency requirements, already apply.

Understanding the risk categories

- **Unacceptable risk:** AI practices presenting a clear threat to people’s safety or fundamental rights are prohibited. Examples include certain forms of manipulation, social scoring and biometric categorisation.
- **High risk:** Systems used in sensitive areas, including recruitment, employment, creditworthiness and some biometric applications, are subject to extensive requirements covering risk management, records and human oversight.
- **Transparency risk:** Systems such as chatbots and some generative AI applications must meet disclosure requirements so that people know when they are interacting with AI or viewing AI-generated content.
- **Minimal or no risk:** Most everyday AI applications fall within this category and are not subject to specific requirements under the Act.
- **General-purpose AI:** GPAI is regulated separately. Most obligations fall on model providers, although firms using these models must still consider how the resulting system is deployed.

When can a UK firm be caught?

The territorial scope of the Act is wider than the location of the organisation using the AI. EU AI Act Article 2(1)(c) covers providers and deployers established or located in a third country, such as the UK, where output produced by the AI system is used in the EU.

The place where the output is used is therefore crucial. A straightforward example might be a UK adviser using an AI system to help prepare an analysis that an EU-based client then uses in its business. The same concern could arise where work produced by a UK team is used by an EU office or group company. It may be less clear where an EU-based client receives advice about a purely UK matter but all material use of the AI output takes place in the UK.

The existence of an EU client, employee or job candidate should therefore prompt investigation, but residence or nationality alone should not be treated as a complete test. In particular, it would be too broad to assume that a UK firm necessarily falls within all the Act's obligations merely because an EU-based candidate applies for a UK role. The firm must consider the precise system, the people affected, where its output is used and which provision is engaged.

This distinction matters because the consequences of overstatement and understatement are both unhelpful. A firm should not ignore an EU connection, but nor should it assume that every piece of AI-assisted work for an EU client is a high-risk activity. Where the position is material or uncertain, specialist advice may be needed.

Client onboarding can provide a useful first alert. Firms could record where the client is based, as well as where the work will be used and whether it will be shared with people or entities in the EU. However, the position can change during an engagement, so the question should also be revisited if the scope or intended recipient of the work changes.

Which uses present the greatest risk?

For most tax advisers, using generative AI to help research a UK tax question or prepare a first draft will not, by itself, make the system high-risk under the EU AI Act. Professional duties remain highly relevant, particularly accuracy, confidentiality, competence, transparency and the exercise of professional judgement, but these should not be confused with the Act's high-risk classification.

The most obvious high-risk area for many professional firms is employment. EU AI Act Annex III includes certain AI systems used to recruit or select individuals, place targeted job advertisements, filter applications, evaluate candidates, allocate tasks based on personal characteristics, or monitor and evaluate workers. If a UK firm uses such a system and its output is used in the EU, it may need to comply with the high-risk regime once the relevant provisions apply.

Not every system used in a listed area is automatically high-risk. The Act contains a limited exception where a system does not pose a significant risk of harm and does not materially influence the outcome of decision-making, although systems that profile individuals remain high-risk. Classification therefore depends on what the tool actually does, rather than the department in which it is used.

Identity verification also needs careful analysis. Remote biometric identification can be high-risk, but systems used solely to confirm that a person is who they claim to be are excluded from the relevant Annex III category. It would therefore be unsafe either to describe every anti-money laundering tool as high-risk or to assume that every tool used in client due diligence is outside the regime. Its functions must be examined.

Other professional work, including tax, corporate finance or audit, does not become high-risk simply because AI is involved. Risk can increase, however, where AI makes or materially influences decisions about individuals, particularly in fields expressly listed in Annex III. Firms should separate two questions: whether the Act applies territorially; and, if so, which obligations apply to the particular system and use.

What does compliance involve?

Where a firm deploys a high-risk system, EU AI Act Article 26 will require appropriate technical and organisational measures to ensure that it is used in accordance with its instructions. Human oversight must be assigned to people with the necessary competence, training and authority. Input data under the deployer’s control must be relevant and sufficiently representative for the intended purpose.

Deployers will also have to monitor operation of the system, keep automatically generated logs under their control for an appropriate period of at least six months and act where they identify a risk or serious incident. Depending on the use, they may have to inform workers and their representatives or tell an individual that a

high-risk system is being used to make, or assist in making, a decision about them. Data protection impact assessment obligations may also be relevant.

EU AI Act Article 50 contains separate transparency requirements. For example, a person interacting directly with an AI system must generally be told that it is AI unless this is obvious from the circumstances and context. A client-facing chatbot should therefore be clearly identified as such.

These are legal obligations, but many overlap with sensible controls that firms should already be considering under data protection law, contractual duties and professional standards. The aim should be a coherent AI governance framework, rather than a separate layer of paperwork created solely for the EU AI Act.

What happens if a firm gets it wrong?

The headline maximum penalties are substantial. Breach of the prohibited practices can attract an administrative fine of up to €35 million or 7% of total worldwide annual turnover for the preceding financial year. Breaches of certain other obligations, including those applying to deployers of high-risk systems and the transparency rules, can attract up to €15 million or 3% of worldwide annual turnover. Supplying incorrect, incomplete or misleading information to notified bodies or national competent authorities in response to a request can attract a fine of up to €7.5 million or 1% of worldwide annual turnover.

Those figures require context. For an undertaking, the turnover-based maximum applies if it exceeds the fixed amount, but the Act provides that an administrative fine imposed on a small or medium-sized enterprise should not exceed the lower of the relevant percentages or fixed sums. Authorities must also consider factors including the nature, gravity and duration of the infringement, whether it was intentional or negligent, mitigation, cooperation, previous infringements and the organisation’s size and economic capacity. The figures nevertheless demonstrate why firms should not leave the issue until a problem occurs.

What should tax practices do now?

The precise obligations depend on the system, its purpose and where its output is used. Firms can nevertheless improve their controls now, helping them identify

possible exposure to the EU AI Act and manage wider professional risks.

1. Know which AI systems are being used

Start with an AI systems register. It should cover generative AI products, meeting assistants, document analysis and tax research systems, client onboarding products, recruitment software and AI functions embedded within existing software. Record the supplier, purpose, responsible person, intended users, data processed and any EU connection.

The register should distinguish between approved tools and those being tested, and record changes in purpose or functionality. It may also uncover ‘shadow AI’: staff using unapproved public tools because they are convenient.

2. Identify where outputs will be used

Build proportionate questions into client and matter onboarding. Where is the client established? Who will receive the work? Will an EU office, group company, authority or individual use an AI-generated output? The answer may not always be known at the outset, so engagement teams should revisit it when the scope changes.

Consider the whole journey of the output, not only the person instructing the firm. A UK parent may commission work that is ultimately used by an EU subsidiary. Recruitment, performance management and group-wide HR tools also deserve particular attention.

3. Classify the use, not merely the product

The same underlying technology can support very different activities. Using a general-purpose tool to suggest headings for a training note is not equivalent to using AI to screen candidates or recommend whether an individual should receive credit.

For each use, record what the AI does, whether it makes or materially influences a decision, who may be affected and whether the output is used in the EU. Check the provider’s documentation rather than relying on a description such as ‘low-risk tool’.

Review the assessment when the tool, data or purpose changes. A system approved for administrative support may create a different risk if it is later used to evaluate

people or generate substantive advice.

4. Keep humans in control

Human oversight should be meaningful. A nominal approval stage is inadequate if the reviewer lacks the time, expertise or authority to challenge the output.

AI-generated tax returns, calculations and advice should be reviewed by appropriately qualified staff before submission or issue. Research should be checked against reliable source material, with citations opened and verified. Reviewers should understand the data and assumptions behind an output rather than checking only whether its conclusion appears plausible.

Identify who may review and approve each type of output and what evidence should be retained. Particularly important advice may justify a second review. A useful working assumption is to treat AI output as work produced by a keen but inexperienced junior: valuable, perhaps, but still requiring supervision, verification and professional judgement.

These controls also reflect the guidance on the application of Professional Conduct in Relation to Taxation to the ethical use of AI, under which members remain responsible for work produced with the assistance of AI tools.

5. Protect information and check providers

Confidential client information, personal data, tax records and payroll information should not be entered into unapproved public AI tools. Firms need clear rules about approved environments and the circumstances in which client consent or disclosure may be required.

Supplier due diligence should cover security, privacy, data location and retention, permitted use of inputs, incident arrangements and access controls. Establish whether prompts or uploaded information will be used to train the provider’s models. For a high-risk system, the firm should also obtain the provider’s instructions covering the system’s capabilities and limitations, its expected accuracy and the human oversight measures required.

The contract should address liability, service continuity and how the firm’s data can be retrieved or deleted when the relationship ends. Material changes may require

reassessment.

6. Be transparent with clients

Firms should decide when and how their use of AI will be disclosed. This may be addressed in engagement letters, terms of business or specific communications where AI plays a significant part in delivering the work. Any consent required under professional standards, contract or data protection law should be obtained and recorded.

Transparency does not mean listing every routine use of automated software. The approach should reflect the tool and the significance of AI to the work. A client should not be misled about who produced substantive advice or exercised professional judgement.

Client-facing chatbots should be clearly identified as AI where required, with an accessible route to a human adviser.

7. Train staff and monitor performance

EU AI Act Article 4 requires providers and deployers to take measures supporting the AI literacy of staff and others using AI systems on their behalf. Staff therefore need practical training on permitted systems, the firm’s rules, confidentiality, hallucinations and escalation routes. Training should reflect their role and the risks of the tool. Recruitment teams will need different guidance from tax staff using a research assistant.

Test outputs before adopting a system and continue to monitor accuracy, bias and quality. This might include recognised tax scenarios and comparisons with trusted sources. Monitoring should also identify use outside the approved purpose and inform decisions about continued use. Keep records of testing and review them periodically as working practices change.

8. Prepare for errors and incidents

Firms should have a clear route for reporting AI errors, unauthorised use, data leakage, misleading outputs and client complaints. Staff need to know when to stop using a system and who to contact.

The response plan should identify who will assess the problem, preserve records, contact the provider and decide whether clients, insurers, regulators or other authorities must be informed. For high-risk systems, the EU AI Act may impose specific notification and suspension requirements.

Incidents and near misses should be reviewed to identify whether the cause lies in the tool or in inadequate instructions, training, access controls or human review. Recording the response will help demonstrate that the firm took its responsibilities seriously.

Preparing for responsible use

AI can save time, reduce cost and improve services, but unexamined use is increasingly difficult to justify. Firms should know which systems they use, where outputs go and which activities need scrutiny, embedding these questions in their wider AI governance.

- Could your use of AI require closer review?
- Does AI make or materially influence decisions about people?
- Is it used to recruit, select, monitor or evaluate workers?
- Are its outputs used by a client, office or other person in the EU?
- Does it process confidential or personal financial information?
- Are its outputs incorporated into tax advice, returns or calculations?
- Are staff using unapproved tools (typically publicly available ones) rather than approved internal AI tools?

One ‘yes’ answer does not necessarily mean that the system is high-risk or that the EU AI Act applies. It is, however, a prompt to investigate and document the position.