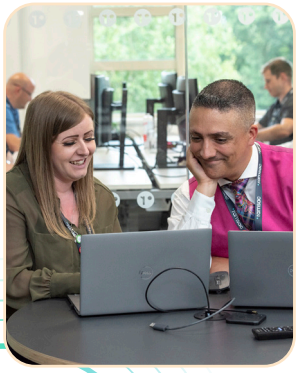








# White paper

## The EU AI Act: What UK organisations need to do now

ramsac
the secure choice

Your Technology. Our Responsibility.

# The EU AI Act

**Artificial intelligence has gone from "nice future concept" to "in everything we do" in a very short space of time.**

Regulation has been scrambling to catch up, and in Europe, it now has. The EU Artificial Intelligence Act ("EU AI Act") is the world's first comprehensive AI law. It became law in all 27 EU member states on 1 August 2024, with obligations phasing in over the next few years.

Even though the UK is no longer in the EU, this law matters a lot for UK organisations, especially anyone selling services into Europe, using EU-based vendors, or handling EU citizens' data.

## Why this matters now

AI is already being used across UK organisations, often embedded inside everyday tools such as HR platforms, finance systems, customer support software, and security products. The EU AI Act is the first law to regulate this reality at scale, and it will apply to many UK organisations whether they realise it or not.

Boards and leadership teams are increasingly being asked simple but uncomfortable questions. Do we know where AI is being used in our business? Could any of it affect people's rights, safety, or livelihoods? And are we confident we could explain and defend those decisions to a regulator, customer, or court?

This paper is designed to help you answer those questions calmly and pragmatically, without turning AI adoption into a compliance headache.

## In this white paper we will explore

- What the EU AI Act actually does
- How and when it will affect UK organisations
- What's happening with UK AI regulation
- A practical action plan for the next 6–18 months

# What the EU AI Act actually does.

## A risk-based law, not a blanket AI ban

The EU AI Act is a risk-based framework that regulates AI according to how much harm it could cause to people's safety, rights, or livelihoods. Broadly, it creates four categories:

### Unacceptable risk - outright banned

These are AI systems considered too harmful to be allowed in the EU. They include:

- Social scoring of individuals (similar to "Black Mirror" reputation systems)
- Emotion recognition in workplaces or schools (Emotion recognition means AI that infers individuals' emotions from facial, vocal, or behavioural data, an approach the EU deems intrusive and unreliable.)
- Certain types of real-time biometric surveillance in public spaces

Because these applications pose a significant threat to fundamental rights, they are banned entirely. **These bans came into effect in February 2025.**

### High risk – heavily regulated, not banned

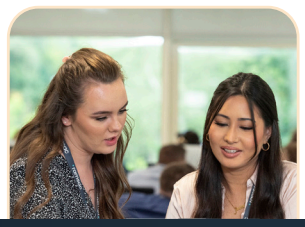
High-risk systems are allowed but subject to strict safeguards because they can meaningfully affect people's lives. Examples are AI used for:

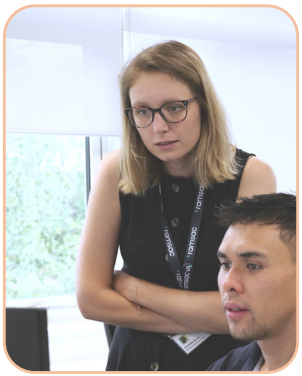
- Recruitment and HR decision-making
- Credit scoring or access to essential services
- Healthcare and medical devices
- Critical infrastructure, education, law enforcement, migration decisions, and democratic processes

Organisations deploying high-risk AI must meet strict requirements, including strong governance and risk management, robust data quality and bias controls with appropriate testing, clear technical documentation and transparency, effective human oversight, and ongoing monitoring with incident reporting.

**Example: HR screening tools**

A UK organisation uses an AI-enabled recruitment platform to score CVs and shortlist candidates. If that system is used for roles filled in the EU, or for EU nationals, it is likely to be classed as high-risk under the EU AI Act. This brings obligations around bias testing, human oversight, documentation, and explainability, even if the tool is bought off the shelf.





### Limited risk – transparency obligations

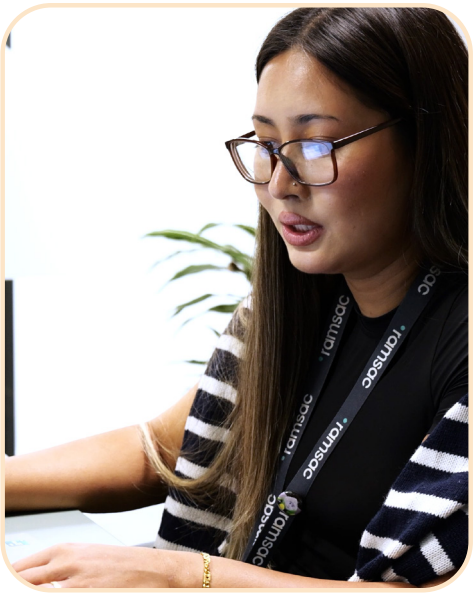
Includes systems like chatbots, where users must be told they're interacting with AI, and tools that generate synthetic images, audio, or video. These systems aren't heavily regulated, but organisations must be clear and upfront about AI involvement so users aren't misled.

**Example: customer scoring and prioritisation**

Many UK organisations use AI-driven scoring to prioritise customers, flag fraud risk, or adjust service levels. Where those scores materially affect access to services, pricing, or outcomes for EU customers, the EU AI Act may apply, and leaders may be expected to justify how those decisions are made.

### Minimal risk – largely unregulated

Covers everyday tools such as spam filters, many recommendation engines, or basic analytics. These systems pose little to no threat to safety or fundamental rights, so they continue to operate under existing laws like data protection and consumer regulations.




## Board takeaway

There are big fines for getting it wrong. Non-compliance can result in penalties of up to €35 million or 7% of global annual turnover, depending on the infringement, similar in scale to GDPR. For many organisations, the bigger risk will be regulatory investigations, forced changes to AI systems, and loss of confidence from customers, partners, and regulators. AI governance is quickly becoming a board-level issue, not just a technical one.

# How and when will it affect UK Organisations

The EU AI Act is not a **"switch it all on tomorrow"** law, it has a staggered implementation timeline:

## Board takeaway

If AI meaningfully affects people, assume higher regulatory expectations and plan governance accordingly.

## 2024

**1 August 2024**
Act entered into force.

## 2025

**2 February 2025**
Bans on unacceptable-risk AI start to apply.

**2025 - 2026**
Obligations kick in for general-purpose AI models (like large language models) around transparency, documentation and, for larger models, cybersecurity and risk management.

## 2026

**2 August 2026**
General date of application: rules for most high-risk AI systems start to apply across the EU.

## 2027

**2027 and beyond**
Further obligations phase in for complex, safety-related and public sector high-risk systems; the framework is expected to be fully effective by 2027–2030, depending on the specific provision.

More recently, the European Commission has been exploring possible delays and grace periods for some high-risk obligations (under political and industry pressure), but the direction of travel is clear: **stricter, risk-based AI regulation is coming, not going away.**

# What's happening with UK AI regulation

So, the main question is... Does the EU AI Act apply to UK organisations? The short answer is: in many cases, **yes, it will.** Like GDPR, the EU AI Act has extraterritorial reach, meaning it can apply to UK organisations that place AI systems or models on the EU market, such as SaaS products, apps, or platforms used by EU customers, or that use AI whose outputs are relied on within the EU, even if the organisation itself is based in the UK. In practice, this means you could be in scope if:

- You offer an AI-powered SaaS product, app, or platform used by customers in the EU
- You operate AI-driven decision-making systems (such as credit, HR, or risk-scoring tools) for EU-based clients
- You are part of a group with EU operations and shared AI tools are deployed across those locations.

If your AI interacts with people in the EU in any meaningful way, it's safest to assume the EU AI Act applies to you.

## What's the UK doing instead?

The UK is taking a "pro-innovation" approach and has explicitly chosen not to copy and paste the EU AI Act. Through its 2023 AI Regulation White Paper and its February 2024 government response, the UK has signalled that it does not plan a single, horizontal AI law in the near term. Instead, it prefers a sector-led, pro-innovation framework where existing regulators (ICO, FCA, CMA, Ofcom, etc.) apply five cross-cutting AI principles in their own domains.

Those regulators are being supported by:

- A new AI Safety Institute, focusing on advanced model safety and testing
- A central government "coordination function" to align regulators on AI risks and standards

## The ICO is already active on AI

The UK Information Commissioner's Office (ICO) has been busy:

- It has detailed guidance on AI and data protection, updated to clarify fairness expectations.
- In April 2024, it published "Regulating AI: the ICO's strategic approach", effectively its roadmap for AI governance and enforcement.

So while there is no "UK AI Act" (yet), UK organisations already have real obligations when they use AI, especially wherever personal data is involved.

## Will the UK eventually legislate?

The UK hasn't committed to AI legislation yet, but it has made it clear that laws may follow if regulators can't keep pace, if gaps appear with key trading partners such as the EU, or if public trust in AI starts to erode. In reality, the most likely outcome is that UK regulation will gradually shift towards EU-style expectations, even if it doesn't mirror the EU approach exactly.

### Board takeaway

- ✓ If you have EU customers or operations > ***start planning.***
- ✓ If AI is used in HR, finance, or decision-making > ***assume scrutiny will increase.***
- ✓ If you rely on vendors' AI > ***you still own the risk.***

# 6–18 month action plan for your organisation

## Step 1: Build an AI inventory

You can't manage what you don't know you're using. Start by cataloging where AI is used across your organisation:

- Off-the-shelf tools (e.g. Copilot, ChatGPT, Google Workspace AI)
- SaaS platforms with embedded AI (CRM, HR, finance, security tools)
- Any in-house models or automations

Note what each system does, what data it uses, and the business impact of its outputs. This becomes the backbone of everything else, the risk assessment, compliance, procurement, and board reporting.


## Step 2: Roughly risk-classify your use cases

You don't need to become an AI lawyer, but you do need to understand which of your AI uses look "higher risk" in EU terms:

- High-impact on people: hiring, promotion, performance management, credit/affordability checks, access to essential services, healthcare decisions, safety-critical operations, law enforcement-style analytics
- Sensitive use of biometrics: face recognition, voice ID, emotion recognition, or biometric categorisation
- Automated decisions with little human review: systems that effectively decide outcomes for people or customers.

Mark these as "likely high-risk" for EU AI Act purposes, and as "high-impact" for your internal risk register.

## Step 3: Stop obviously problematic use cases

The EU AI Act bans certain types of AI outright, and frankly, most organisations shouldn't want to be anywhere near them anyway. Review whether you (or your suppliers) are using, or planning to use:

- Emotion recognition for staff monitoring or student evaluation
- Social scoring or "reputation scores" that aggregate people's behaviour across contexts
- Predictive policing-style profiling of individuals
- Unconstrained real-time facial recognition in public spaces

If anything in your roadmap resembles this, it should be removed or redesigned immediately. Even where it's technically legal in the UK today, it's likely to become a reputational and regulatory liability.

## Step 4: Integrate AI into your data protection & risk processes

For anything touching personal data (which is most modern AI):

- Update or create Data Protection Impact Assessments (DPIAs) that explicitly consider AI-specific risks (bias, explainability, repurposing of data, large-scale profiling).
- Use the ICO's AI and data protection guidance and its explainability resources as your baseline.
- Make sure AI-related risks are logged in your corporate risk register and, where relevant, into frameworks like ISO 27001, Cyber Essentials Plus, or your ISMS.

## Step 5: Tighten up AI-related vendor management

Your AI risk is often shaped by the AI risks within your supply chain, so understanding how vendors use AI is critical. For key AI-enabled suppliers, request a clear explanation of how their AI works, what it is used for, and whether they believe it could fall under the EU AI Act's high-risk category. You should also expect evidence of data-protection compliance, sound AI governance, and appropriate security and incident-handling measures, particularly for GPAI providers. Where contracts are being renewed, build in:

- Obligations on transparency, documentation, and cooperation around AI
- Explicit allocation of responsibilities for EU AI Act and data-protection compliance
- Audit / assurance rights, especially for high-risk or business-critical AI.

## Step 6: Put basic AI governance in place

You don't need a 100-page AI policy, but you do need some structure. As a minimum, you should assign ownership, an AI lead or committee spanning IT, security, data protection, and the business. You should also create a short, practical AI policy covering:

- Approved / prohibited tools
- Rules on using generative AI with company or client data
- Requirements for human review of high-impact decisions
- Expectations for testing and sign-off before deploying new AI use cases

Align that policy with the EU's risk-based approach and with the UK's AI principles and existing regulatory guidance, particularly from the ICO.

## Step 7: Train your people (and not just the techies)

Human behaviour will make or break any AI strategy, so staff need clear guidance on how AI is used in your organisation, what they can and can't do with AI tools, and the risks of feeding confidential, personal, or commercially sensitive data into public systems. Managers should also be trained on how to question AI-assisted decisions and when they are required to override them. For regulated sectors such as financial services, healthcare, or the public sector, AI training should be tied directly to existing regulatory obligations.

# AI literacy, a growing regulatory expectation

The EU AI Act introduces an explicit requirement for organisations to ensure an appropriate level of AI literacy among staff who design, deploy, manage, or rely on AI systems. This obligation is expected to apply across EU organisations as the Act reaches general application by mid-2026.

AI literacy does not mean teaching everyone how AI models work. It means ensuring people understand when AI is being used, the limitations and risks of those systems, and their responsibility to question, challenge, and override AI-assisted decisions where necessary.

While the UK has not mandated AI literacy in law, UK regulators are already moving in this direction through guidance on accountability, fairness, and explainability. For UK organisations, particularly those with EU customers or operations, building AI literacy should be seen as best practice rather than a future compliance burden.

Organisations that invest early in proportionate AI training for staff, managers, and leaders will be better placed to meet future regulatory expectations, build trust, and avoid over-reliance on systems they do not fully understand.

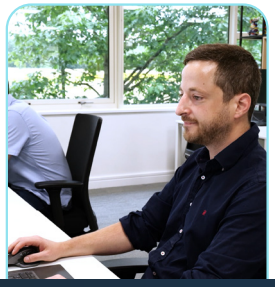
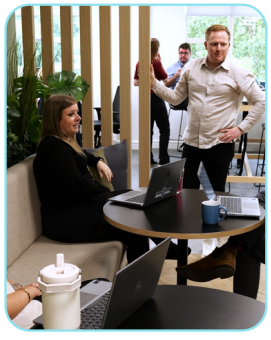
# Why starting now makes sense.

Even if you're not yet sure whether you fall within the scope of the EU AI Act, and even though the UK has not introduced its own AI legislation, the actions outlined in this white paper represent **good digital governance** that all organisations should undertake. Getting ahead now will:

- Reduce the cost and disruption of future compliance (EU or UK)
- Build trust with customers, staff, regulators, and partners
- Make it easier to adopt new AI tools quickly and safely
- Avoid nasty surprises when regulators or clients ask for your AI risk framework

If you're already doing serious work on GDPR, cyber security, and information governance, this isn't a whole new universe, it's the next logical step.



# When should you get help?

You may not need external support if AI use in your organisation is limited, low-impact, and well understood. You should consider specialist help if any of the following are true:

**You can't confidently list where AI is being used across the business.**

**You have EU customers, partners, or group entities.**

**AI is involved in hiring, performance management, customer scoring, or access to services.**

**Your board is asking questions that currently rely on assumptions rather than evidence.**

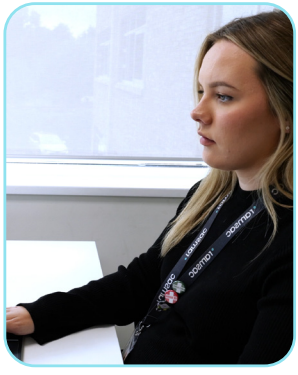
# Where to go from here.

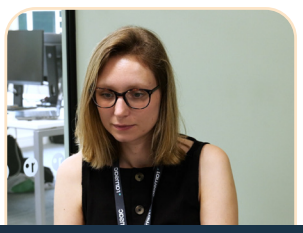
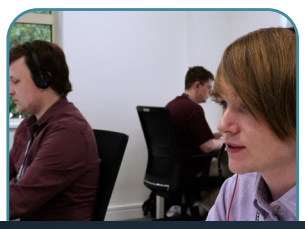
A sensible sequence for most UK organisations over the next 6–12 months is:

- ✓ **Create an AI inventory and risk map**
- ✓ **Identify high-impact / likely high-risk use cases**
- ✓ **Align with ICO guidance and your existing GDPR / security framework**
- ✓ **Update procurement, contracts and policies to reflect AI-specific risks**
- ✓ **Develop a simple AI governance structure and training programme**
- ✓ **For organisations with EU customers or operations, start planning towards EU AI Act compliance for any AI that could be in "high-risk" territory**

If you'd like to turn this into a more detailed roadmap for your business, or sense-check where you are today, this is exactly the sort of thing your IT and governance partners (like a good MSP) should be helping you with.






ramsac
the secure choice

# About ramsac

Since 1992, ramsac has been helping organisations thrive with secure, reliable technology.

We are proud to be different. We are a people-first business, committed to making IT simple, jargon-free and friendly. We are independent consultants, offering advice based on your needs, not on sales targets. And we are focused on long-term relationships, with many clients trusting us for over 20 years.

Our commitment to quality is backed by ISO 9001, ISO 27001 and Cyber Essentials Plus certifications, and we are proud winners of multiple national and regional business awards. Most importantly, we have been recognised as a Best Companies 3 Star World Class Employer, proof that our team love what they do, and that passion shows in the service we deliver.

## Unsure where your AI risks sit?

If you want help understanding how the EU AI Act and UK guidance apply to your organisation, we can help you assess your current AI use, identify high-risk areas, and define clear next steps.

Speak to us about a practical starting point.
Call **01483 412040**, **email** **info@ramsac.com** or visit **www.ramsac.com**

ramsac
the secure choice