SEPTEMBER 2026

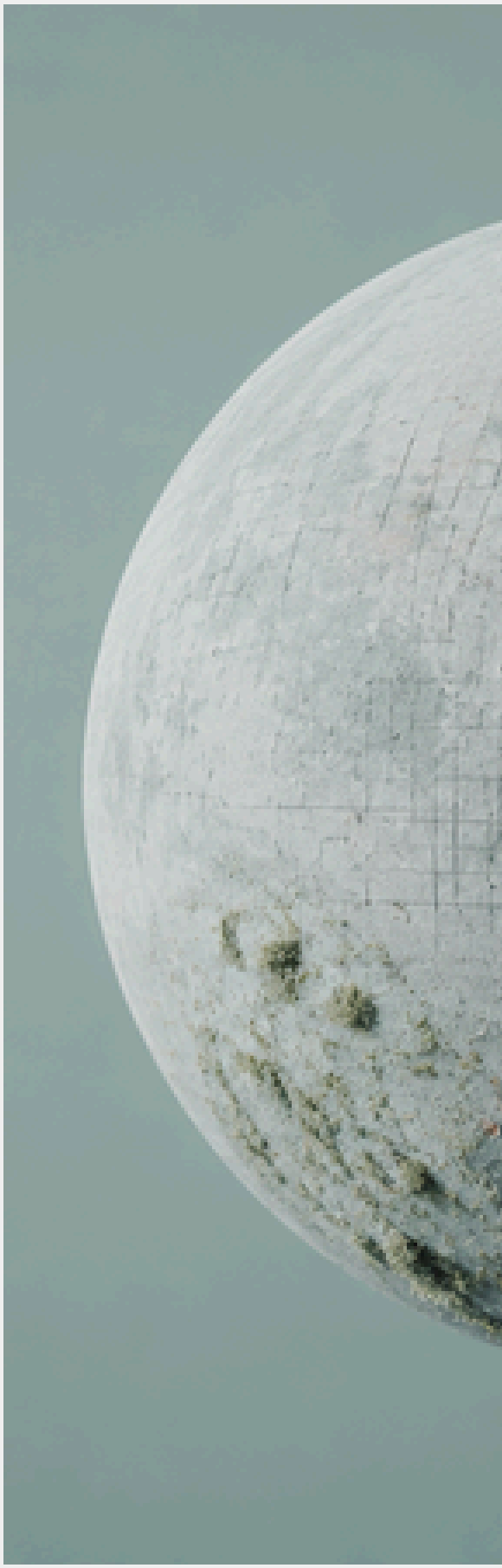
EU AI ACT

Business Guide and Compliance Checklist

A PRACTICAL RESOURCE FOR UK PROFESSIONAL SERVICES ORGANISATIONS

calls9

TABLE OF CONTENTS



calls9

01

THE EU AI ACT AT A GLANCE

The EU AI Act is the European Union's legal framework for artificial intelligence. It creates a common set of rules for the development, supply and use of AI within the EU and takes a risk-based approach, with stricter requirements applying to AI systems that can create greater risks to safety or fundamental rights.

The Act applies to both public and private organisations and can apply to organisations established outside the EU where they place an AI system or general-purpose AI model on the EU market, put an AI system into service or use it in the EU. The legislation also contains specific provisions covering providers and deployers outside the EU where an AI system's output is used within the EU.

FOUR THINGS BUSINESSES NEED TO UNDERSTAND

1. What AI are you using?

You need a clear view of the AI systems used across your organisation before you can determine which rules may apply. Classification under the AI Act depends on factors including the system's intended purpose and how it is used.

2. What is your role?

The AI Act creates different responsibilities for different operators, including providers and deployers of AI systems.

3. What level of risk applies?

The Act uses a risk-based model. It covers prohibited AI practices, high-risk systems, AI subject to transparency requirements and systems presenting minimal or no additional risk under the AI Act.

4. What other rules apply?

The EU AI Act does not replace other legal or professional duties. For UK organisations processing personal information through AI, UK data protection requirements can still apply. The ICO provides specific guidance on applying UK data protection principles to AI systems.

DISCLAIMER

This guide provides general information and is not legal advice. The requirements that apply will depend on the specific AI system, your organisation's role, how and where the system is used and any sector-specific duties. Check current official guidance and seek specialist advice where required.

02

EU AI ACT IMPLEMENTATION TIMELINE

The AI Act is being introduced in stages. The current timetable reflects the amendments introduced by the Digital Omnibus on AI in July 2026.

1 AUGUST 2024

AI Act enters into force

The AI Act formally entered into force on 1 August 2024.

2 FEBRUARY 2025

First rules start applying

The rules covering AI definitions, AI literacy and prohibited AI practices started to apply.

2 AUGUST 2025

General-purpose AI and governance

Obligations for providers of general-purpose AI models started to apply. EU governance arrangements also had to be established and Member States were required to designate competent authorities.

27 JULY 2026

Digital Omnibus on AI enters into force

The Digital Omnibus on AI amended the AI Act, including extending the timetable for high-risk AI requirements and simplifying some administrative requirements.

2 AUGUST 2026

Most rules apply and enforcement begins

The majority of applicable AI Act rules reached their main application milestone. Article 50 transparency requirements also started to apply, and enforcement began for applicable rules at EU and national level.

calls9

IMPORTANT

Older EU AI Act guidance may contain the original 2026 and 2027 high-risk deadlines. Organisations should use the current European Commission implementation timetable when planning compliance.

View European Commission AI Act Service Desk: Current implementation timeline

03

HOW THE EU AI ACT CLASSIFIES RISK

Not every AI system faces the same requirements. Classification depends on the intended purpose of the system and the context in which it is used.

Prohibited AI practices

A limited group of AI practices are prohibited. These include certain forms of harmful manipulation and exploitation, social scoring, untargeted scraping of facial images, some emotion recognition in workplaces and education, and certain biometric categorisation practices.

High-risk AI

Some AI systems are treated as high-risk because of their potential impact on people's safety or fundamental rights. Examples include certain systems used for recruitment and employee management, education, access to essential services, biometrics and other sensitive use cases listed in Annex III.

AI with transparency requirements

Article 50 creates transparency duties for certain interactive and generative AI systems. This includes requirements concerning direct interaction with AI, machine-readable marking of some AI-generated material, deepfakes, emotion recognition and biometric categorisation.

Minimal or no additional AI Act risk

The European Commission states that the majority of AI systems can be developed and used under existing legislation without additional legal obligations under the AI Act's stricter risk categories.

04

WHAT DOES THE EU AI ACT MEAN FOR UK ORGANISATIONS?

The short answer: ***it can apply.***

The AI Act can apply to organisations established outside the EU. This includes organisations that place an AI system or general-purpose AI model on the EU market, put an AI system into service or use it in the EU. The Regulation also covers certain providers and deployers established outside the EU where the output produced by their AI system is used within the EU.

Example 1: You provide AI into the EU

A UK company providing an AI system to customers in EU countries may fall within the scope of the Act even though the business itself is established in the UK.

Example 2: AI output is used in the EU

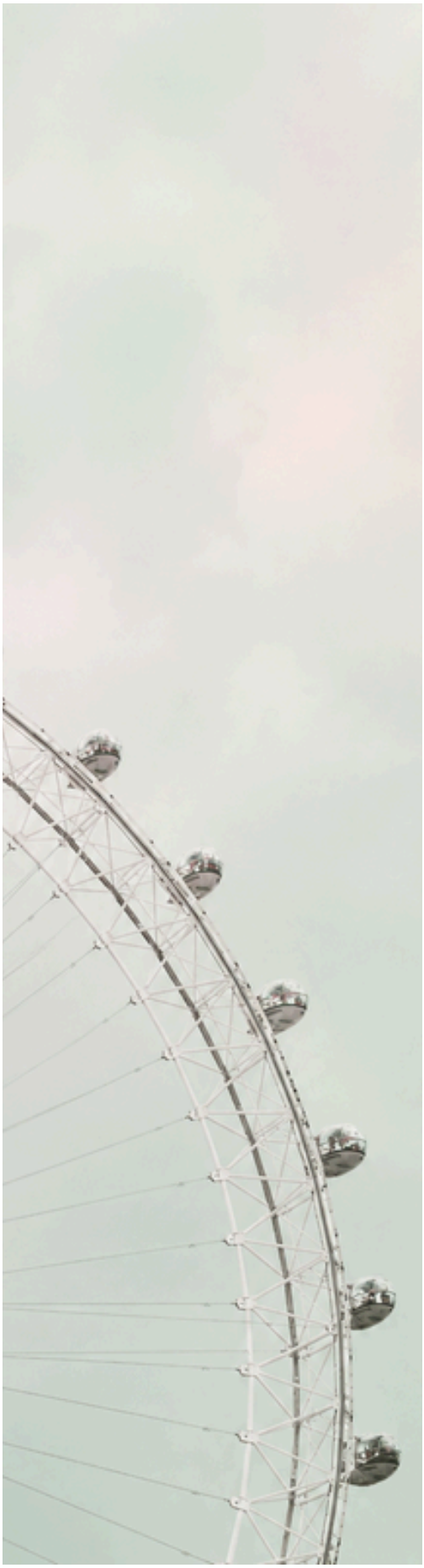
The Act contains provisions applying to providers and deployers in third countries where AI system output is used in the EU.

Example 3: You use AI only within the UK

Using AI solely within a UK operation does not, by itself, automatically bring the organisation within the EU AI Act. UK data protection requirements and professional or sector-specific duties may still apply.

Four questions to ask first

1. Where is the AI system provided or used?
2. Where are its users, clients and affected individuals?
3. Where is its output used?
4. What personal, confidential or commercially sensitive information does it process?



calls9

Build a responsible AI strategy

Introducing the AI Fast Lane Programme by Calls9

AI Fast Lane helps you identify where AI can create the most value across your organisation, while making sure governance, data protection, security and regulatory requirements are considered from the start.

We work with your team to understand your current position, define the right opportunities and build a practical AI strategy that supports responsible adoption and delivery.

- Audit your existing AI capabilities
- Create your generative AI strategy
- Identify generative AI use cases
- Build and deploy GenAI solutions
- Testing and continuous improvement

Achieve end-to-end AI transformation

Book a free consultation

05

WHY PROFESSIONAL SERVICES FIRMS SHOULD LOOK BEYOND THE AI ACT

For professional services firms, AI governance is not only about AI-specific regulation.

Many firms handle confidential client and employee information, personal data, commercially sensitive documents and other information subject to professional duties. The relevant obligations will depend on the profession and the work being carried out.

For example, the Solicitors Regulation Authority requires regulated solicitors and firms to keep the affairs of current and former clients confidential unless disclosure is required or permitted by law or the client consents.

ICAEW's Code of Ethics also places confidentiality duties on professional accountants. ICAEW's July 2026 guidance specifically advises firms to consider how confidential information is protected when using AI, including where information is stored, who can access it and whether it may be used to train models.

Professional Conduct in Relation to Taxation guidance also states that client confidentiality extends to the use of AI. It warns that entering client data into publicly available AI tools is likely to breach client confidentiality unless the client has consented, and recommends anonymising information used with public AI systems.

This is why a useful AI checklist for professional services needs to consider regulation, client duties, data protection, professional judgement, supplier risk and information security together.

EU AI ACT READINESS CHECKLIST FOR UK PROFESSIONAL SERVICES

Use this checklist to review significant AI systems and use cases individually. It combines EU AI Act requirements that may apply, UK data protection considerations, examples from professional body guidance and practical security controls.

Not every item will create a legal duty for every organisation. This checklist is designed primarily for organisations deploying and using AI. If you act as a provider, importer or distributor, additional AI Act obligations may apply.

A. KNOW WHAT AI YOU USE AND WHERE

1. Create a complete AI inventory

Record all AI systems used or provided by the organisation, including standalone tools, AI features built into existing software, client-facing AI and tools purchased directly by individual teams. Prioritise systems for detailed review based on their purpose, data and potential impact.

2. Record the purpose of each AI system

Document what each system does, which business process it supports, who uses it and who can be affected by its output.

3. Identify your role for each system

Establish whether your organisation acts as a provider, deployer, importer, distributor or another operator.

4. Map where the system and its outputs are used

Record where your organisation, users and clients are based and where AI outputs are used.

5. Assign an internal owner

Record who is responsible for the business use, supplier relationship, data and risk associated with each significant system.

Good practice: *The ICO's AI guidance places strong emphasis on accountability, documented responsibilities and governance for AI processing personal information.*

B. PROTECT CLIENT INFORMATION AND PERSONAL DATA

6. Identify what information enters the AI system

Check whether prompts, uploaded documents or connected systems contain:

- personal information;
- special category information;
- criminal offence information;
- client-confidential information;
- legally privileged material;
- commercially sensitive information;
- intellectual property belonging to your organisation, clients or third parties.

Why: UK data protection principles apply where personal information is processed, while professional confidentiality duties can apply separately.

---

7. Set clear rules for confidential information

Define what staff may and may not enter into public or externally hosted AI tools.

For accountancy and tax professionals, current ICAEW and PCRT guidance specifically addresses the need to protect client information when using AI and warns against placing identifiable client information into public AI tools without the necessary authority and protections.

---

8. Check the lawful basis for personal data processing

Where AI processes personal information, identify why that processing is lawful and whether further conditions are required for special category or criminal offence information.

Why: The UK GDPR requires an appropriate lawful basis for processing personal data and additional conditions can apply to more sensitive categories of information.

---

9. Decide whether a Data Protection Impact Assessment is required

Assess whether an AI project is likely to create a high risk to individuals.
A DPIA is required under UK data protection law where processing is likely to result in high risk. The ICO states that a DPIA is always required for systematic and extensive profiling or automated evaluation used for decisions producing legal or similarly significant effects.

10. Review privacy information

Check whether privacy notices accurately explain how AI is being used where personal information is involved.

Why: UK data protection law requires organisations to process personal data transparently and to be clear about how and why information is used.

---

11. Check international data transfers

Identify whether personal information is transferred or accessed outside the UK through the AI supplier, model provider, cloud platform or sub-processors.

---

12. Review retention, deletion and access

Understand whether prompts, uploaded files, outputs and logs are stored, for how long and who can access them.

Why: UK data protection principles include data minimisation, storage limitation, security and accountability.

C. CHECK AI RISK, TRANSPARENCY AND PROFESSIONAL JUDGEMENT

13. Check for prohibited AI practices

Review each significant use case against the current Article 5 prohibited practices.

Why: The original prohibitions have applied since 2 February 2025. Additional prohibitions introduced by the Digital Omnibus apply from 2 December 2026.

---

14. Check whether any system may be high-risk

Pay particular attention to AI involved in recruitment, employee management, access to essential services and other Annex III areas. The AI Act specifically lists certain employment-related uses, including analysing and filtering job applications and evaluating candidates, as high-risk use cases.

---

15. Review automated decisions about people

Identify any system that automatically makes, recommends or materially influences decisions about employees, candidates, clients or other individuals.

Where UK personal data is involved, specific protections apply to certain solely automated decisions producing legal or similarly significant effects, including rights relating to human intervention and challenging decisions.

16. Build human review into professional work

Define which AI outputs require review by a suitably qualified person before they inform advice, decisions, client communications or final deliverables.

Professional bodies have warned that AI output can be inaccurate and that professional responsibility remains with the human professional. ICAEW guidance for tax professionals says AI does not replace professional judgement, while the SRA highlights the need to manage AI errors and supervise its use in legal services.

17. Define how AI output will be checked

Set checks appropriate to the use case, such as verifying facts, calculations, cited sources, legal authorities and conclusions before the output is relied on.

The ICO advises organisations to consider statistical accuracy and the effect incorrect AI inferences can have on individuals and decisions. The NCSC also warns that generative AI can confidently produce incorrect statements.

18. Check AI transparency requirements

Review AI systems that interact directly with clients or other individuals and any use of AI-generated text, audio, images or video.

Article 50 transparency rules apply from 2 August 2026. They cover direct interaction with AI and specific types of AI-generated or manipulated content, with detailed exceptions and requirements set out in the Commission's guidance.

19. Check recruitment and HR AI separately

Do not treat HR tools as ordinary productivity software. Review AI used to advertise roles, screen CVs, rank candidates, evaluate employees or support employment decisions.

Certain recruitment and worker-management AI systems are listed as high-risk under Annex III.

D. REVIEW SUPPLIERS, CONTRACTS AND SECURITY

20. Carry out AI supplier due diligence

For significant systems, understand:

- which model or models are used;
- where information is processed and stored;
- whether your data may be used for training;
- what sub-processors are involved;
- what security controls are in place;
- how model or system changes are managed;
- what documentation the supplier provides;
- how incidents are reported;
- what happens to your information when the contract ends.

ICAEW's 2026 confidentiality guidance specifically advises firms using AI to understand where client data is stored, who can access it and whether it may be used to train models.

---

21. Review controller and processor responsibilities

Where personal information is involved, establish which organisation determines the purposes and means of processing and make sure contracts reflect the actual relationship.

The ICO recommends that contracts with AI suppliers clearly identify controller and processor roles, processing responsibilities, sub-processors and agreed technical and organisational controls.

---

22. Review client engagement terms where appropriate

Consider whether engagement letters, terms of business or client-facing policies should explain the use of AI in service delivery, particularly where client data will be processed by AI systems.

ICAEW updated its 2026 engagement letter guidance to cover the use of AI, including whether AI will be used in service delivery, limitations of the tools and responsibilities for data protection, confidentiality and supplier due diligence.

23. Apply appropriate access controls

Give users and AI systems access only to the information and systems required for their role and use case.

The NCSC recommends limiting AI system permissions and applying least-privilege access, particularly for agentic AI that can take actions across connected systems.

24. Include AI in security and incident planning

Consider prompt injection, unauthorised disclosure, compromised integrations, data poisoning, inappropriate system actions and supplier incidents in your security planning.

The NCSC identifies AI-specific security risks alongside existing cyber threats and recommends treating security as a requirement throughout the AI system lifecycle.

E. PUT GOVERNANCE AND PEOPLE AROUND AI

25. Create an approved AI policy

Give employees clear rules covering:

- approved AI systems;
- prohibited uses;
- client and personal information;
- confidential information;
- human review;
- use of AI-generated content;
- escalation of concerns;
- reporting of errors or incidents.

This supports wider accountability and helps organisations put AI literacy into the context of how AI is actually used in their business.

26. Provide role-based AI literacy

Train people according to what they actually do with AI.

The current Article 4 requires providers and deployers to take measures supporting AI literacy while considering factors such as people's technical knowledge, experience, education, training and the context in which systems are used. The Commission states that there is no single mandated level of AI literacy and no requirement for a specific certificate.

27. Train people responsible for human oversight

If the organisation deploys high-risk AI, make sure people responsible for human oversight have the necessary competence, training, authority and support. This becomes a specific deployer duty when the relevant high-risk requirements apply to your system. Prepare ahead of the applicable deadline.

28. Keep evidence of your decisions

Maintain records covering:

- the AI inventory;
- risk classification;
- approved and rejected use cases;
- data assessments;
- DPIAs where required;
- supplier reviews;
- training;
- policies;
- testing and review;
- incidents;
- significant changes to systems or use cases.

Once the relevant high-risk requirements apply to your system, deployers must meet specific record-keeping and monitoring duties. This includes retaining automatically generated logs under their control for at least six months, unless another applicable law provides otherwise.

29. Review systems when something changes

Repeat the relevant assessment when there is a significant change to the AI system, supplier, model, data, purpose, user group or business process. AI systems and associated risks can change over time. The ICO advises that DPIAs should be treated as living documents and reviewed when the nature, scope, context or purpose of processing changes.

07

ADDITIONAL CHECKS IF YOU USE HIGH-RISK AI

If your assessment identifies a system that falls within the AI Act's high-risk category, additional requirements can apply.

Deployers of high-risk AI systems are required to use systems in line with the provider's instructions, put appropriate human oversight in place, monitor operation and respond to identified risks or serious incidents.

- Where input data is under the deployer's control, deployers of high-risk systems must ensure that it is relevant and sufficiently representative in view of the system's intended purpose.

- Where a high-risk system is used in the workplace, the AI Act includes requirements to inform affected workers and workers' representatives before the system is put into use.

- Where a high-risk AI system is used to make or assist decisions about natural persons, additional information obligations can also apply to affected individuals.

A fundamental rights impact assessment is not required of every private business using high-risk AI. The requirement applies to specified deployers, including bodies governed by public law, private entities providing public services and certain deployers involved in creditworthiness or life and health insurance risk assessments.

08

YOUR PRIORITY ACTIONS

After completing the checklist, identify the areas requiring action.

IMMEDIATE

What needs to change now?

NEXT 90 DAYS

What should be improved or put in place?

LONGER TERM

Which systems or processes need further review before the 2027 and 2028 high-risk deadlines?

OWNER

Who is responsible for taking this work forward?

Use compliance to support better AI decisions

AI governance should not only help your organisation respond to regulation.
A clear understanding of your AI systems, data, suppliers, risks and responsibilities can also help you make better decisions about which AI opportunities are worth investing in.

EXECUTIVE SUMMARY

The EU AI Act is now a practical business issue, not simply a future regulatory concern. Many of its provisions apply from August 2026, while further requirements for high-risk AI will follow in 2027 and 2028.

For UK professional services firms, the key question is not simply whether the organisation is based in the EU. The Act can apply depending on how AI is provided, where it is used and where its outputs are used.

A practical response starts with understanding your own AI use.

- Know which AI systems and tools are being used across the organisation.
- Understand your role and whether the EU AI Act applies to each significant use case.
- Identify prohibited, high-risk and transparency-related uses.
- Protect client information, personal data and confidential material.
- Review suppliers, contracts, security and data handling.
- Put clear human review around professional advice and important decisions.
- Give teams practical AI guidance and role-based training.
- Assign ownership and keep evidence of assessments, decisions and actions.
- Review your position as AI systems, suppliers and regulation change.

The aim should not be compliance for its own sake. A clear approach to AI governance can help organisations reduce risk while making better decisions about where and how AI should be used.

calls9

Make compliance part of your AI strategy

Build and adopt AI responsibly with the AI Fast Lane Programme

AI adoption brings new opportunities, but also new questions around regulation, data, security, governance and risk.

AI Fast Lane helps you address these as part of your wider AI strategy. We assess how AI is being used, identify where it can create business value and help you put the right policies, controls and ways of working in place as you move into delivery.

- Audit your existing AI capabilities
- Create your generative AI strategy
- Identify generative AI use cases
- Build and deploy GenAI solutions
- Testing and continuous improvement

Achieve end-to-end AI transformation

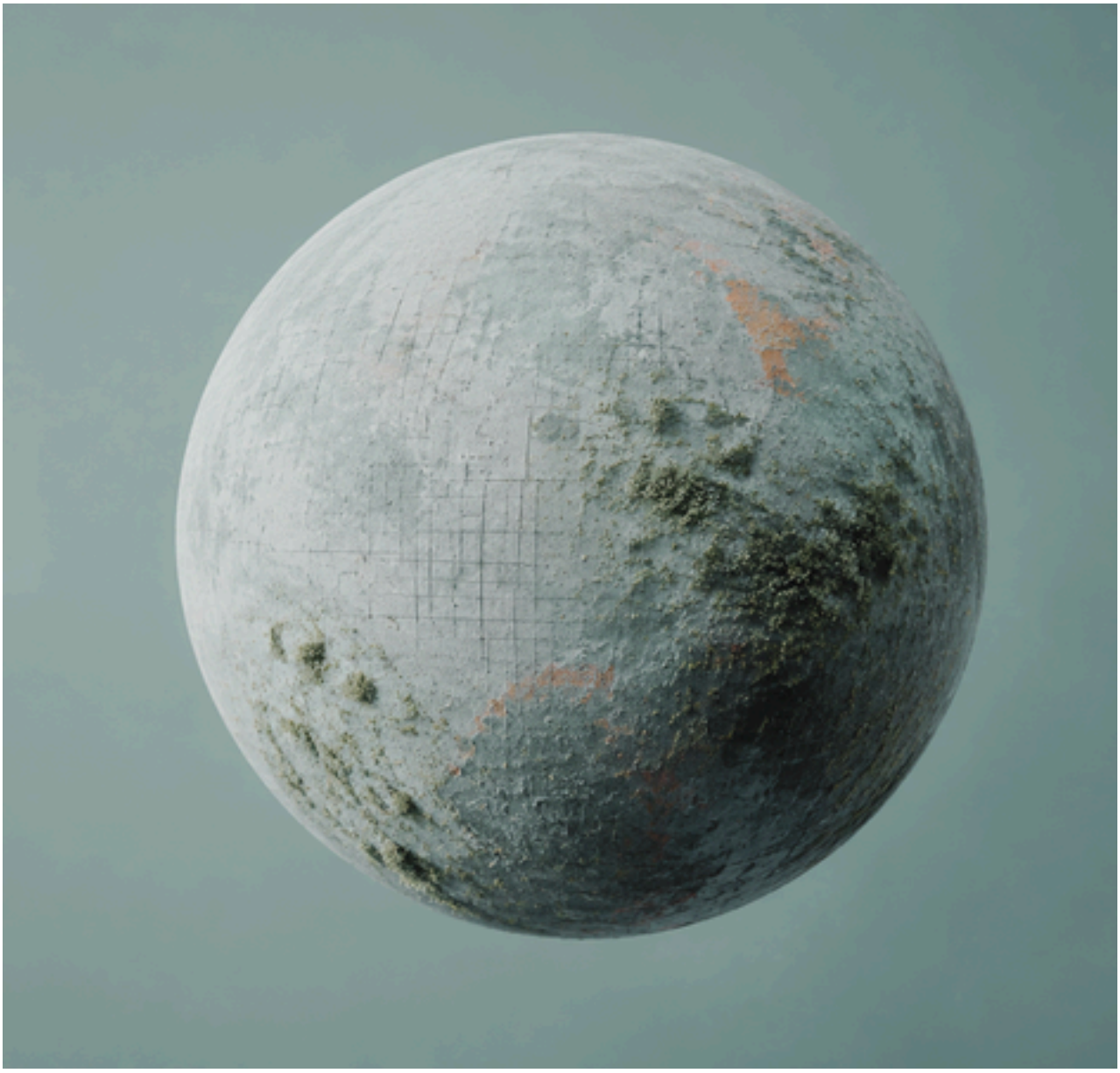
Book a free consultation

CONTINUE READING

This checklist accompanies our article EU AI Act 2026: What UK Businesses Need to Know and Do Now, which explains what changed in 2026, why the Act matters to UK organisations and the key questions business leaders should be asking.

Read the full EU AI Act 2026 article →

Use the article for the wider context, then use this guide and the EU AI Act Readiness Checklist for UK Professional Services to assess your organisation's current position and turn identified gaps into practical actions.



Who we are

Calls9 is a **Digital Innovation and Transformation Agency**. We specialise in designing and building world-class digital products and services. Our unique approach builds a team of digital experts around your needs and budget. Acting as a stand-alone team or an extension of yours, we partner to solve your digital challenges at speed.

Our services

- AI Fast Lane Programme
- Digital Product Design and Development
- Web3 Development
- Legacy System Modernisation
- Innovation Consultancy
- Website and App Development

Get in touch

www.calls9.com

hello@calls9.com

+44 (0) 113 350 6441

linkedin.com/company/calls9/

calls9