

ICO secures data protection changes from ten AI developers and opens agent inquiry

Source copy kept by wheresthe.ai for the story "ICO secures data protection changes from ten AI developers and opens agent inquiry" (<https://wheresthe.ai/d/gb-ico-foundation-model-developers-agents-2026-10/>).

Source: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/10/ico-secures-changes-from-leading-ai-developers-as-scrutiny-extends-to-ai-agents/>

Text saved 18 Oct 2026 (the page as published).

SHA-256 of the saved text: 88ebd564117d3746b55387fab7f7bc4c6451ccd8ac7c3c222303d5dc3124afe0

ICO secures changes from leading AI developers as scrutiny extends to AI agents

Date 8 October 2026

Type News

Ten leading AI foundation model developers have made, or committed to make, changes following supervision in new report.

We launch a call for evidence on data protection risks of agentic AI.

Regulator confirms enquiries around recent agentic AI testing and deployment earlier this year.

We have secured data protection improvements from ten of the world's largest AI foundation model developers in a new report published today.

It comes as we launch a call for evidence on agentic AI and confirm enquiries around recent agentic AI testing, marking the next phase in its work to regulate the technology.

Industry improvements to foundation models

From chatbots to assistants, many AI tools are powered by a relatively small number of foundation models. They are trained on large volumes of personal data and can be adapted for different purposes.

Following scrutiny from us, ten of the biggest foundation model developers operating in the UK - Amazon, Anthropic, Apple, Cohere, DeepSeek, Google, Meta, Microsoft, OpenAI and Stability AI - have made, or committed to make, data protection changes.

These included clearer transparency information, stronger mechanisms for people to exercise their rights and tougher assessments of safeguards. We are monitoring developers' progress against their commitments.

The report also sets out our regulatory positions on key issues, including how special category data can be used lawfully and whether foundation models themselves may contain personal data.

We acknowledge that current foundation model training practices present technical challenges when it comes to complying with UK data protection law and data protection by design principles. We are proactively raising these boundaries of the law with Government, as addressing them will require ongoing collaboration between industry, regulators and Government as the technology continues to evolve.

The rise of AI agents

Foundation models underpin a new wave of AI agents capable of completing tasks, using tools and interacting with websites, often with limited human oversight.

As these systems become more autonomous, the data protection risks are evolving - from questions about how AI systems are trained to how they might behave independently once deployed.

Richard Nevinson, Director of Technology Regulation at the ICO, said:

AI has huge potential to benefit our society, but that depends on trust and transparency. Our engagement with some of the biggest developers has secured real commitments that will help people better understand and control how their data is used, even in a fast-moving and complex area. But as AI systems operate with greater autonomy, robust data protection safeguards become even more critical.

Next steps

We have today launched a six-week call for evidence, seeking views from developers, deployers and other experts on how organisations are managing the data protection risks of agentic AI.

We have recently made enquiries with OpenAI, Anthropic, Meta and the UK's AI Security Institute around recent agentic AI testing and deployment.

In some cases, certain agents reportedly bypassed protections, used unauthorised communication channels and accessed external systems such as Hugging Face, raising potential concerns about safeguards, accountability and oversight.

Richard Nevinson added:

These recent reports show both how fast these systems are advancing, and the risks they pose if the guardrails aren't fit for purpose. Our message is clear: the fact AI agents act with autonomy is not an excuse for poor compliance. If people are to trust AI innovation, they rightly expect to know how their personal information is being protected.

The evidence gathered from the call will inform our future guidance, providing greater clarity to organisations and supporting them to innovate responsibly while protecting people's rights. It will also support the development of our forthcoming statutory code of practice on AI and automated decision-making.

Another priority area for us is the increasing personalisation of consumer-facing AI services, such as popular general-purpose chatbots and chatbots used for role-play and companion purposes.

We are conducting research with the public to understand any concerns and engaging with firms to ensure that their products meet people's needs in a transparent and privacy-focused way.

Promoting trust and transparency in AI is a regulatory priority for us in our corporate strategy, which was recently open for consultation .

Respond to the call for evidence by 20 November 2026.

[Click to toggle details](#)

Notes to editors

The ICO's enquiries into reported agent testing incidents are ongoing.

The ICO has contacted several developers and their testing partners to establish what risk assessments and safeguards were in place at the time.

The call for evidence covers security, transparency, accountability, automated decision-making, fairness and lawful data use.

Earlier this year, the ICO set out its early thinking on agentic AI in its Tech Future report , including the potential uses, data protection implications and expected technical developments.

In 2025, the ICO established a dedicated foundation model policy and supervision programme under its AI & Biometrics Strategy. The programme ran over two years and covered 11 priority developers, identified by likelihood of non-compliance, UK market share, and use of higher-risk training datasets.

The ICO paused its engagement with X.AI after it opened a formal investigation into the Grok AI system, leaving ten developers. This investigation is ongoing.

More information on the ICO's work on AI here .

The legal entity is now known as the Information Commission. The organisation is now referred to as the Information Commission's Office, or ICO. Under new governance arrangements introduced by the Data (Use and Access) Act 2025, the work of the ICO is now overseen by a new Information Commission Board. The transition has moved the ICO from a corporation sole (the Information Commissioner) to a collective decision-making Board.