A&O SHEARMAN

OPINION

The future of agentic AI and its data protection implications: the UK ICO's initial assessment

FROM OUR BLOG

A&O Shearman on data

READ TIME

7 mins

PUBLISHED DATE

Jan 22 2026

Agentic AI heads towards the mainstream

As the democratisation of AI continues apace, organisational deployment of AI agents is rapidly becoming a reality. To take one example, in September last year OpenAI announced the launch of Instant Checkout and the Agentic Commerce Protocol, (developed with Stripe), which will enable integration for AI chat engagement and purchasing within a single application. This is an early development in what we expect will define future paradigms of AI shopping experiences, and AI agents will have similarly transformative effects in many other sectors.

Agentic AI will pose challenges across many legal spheres, including liability, IP and contractual law. In addition, it will be key to address questions about data protection when looking to mitigate risks to individuals, and to enable responsible innovation and benefits the technology will offer. A&O Shearman is advising many of the world's largest businesses on the pioneering transactions and governance needed for the adoption of AI agents.

First data protection regulatory report

In January 2026, and in the context of recent technological developments, industry announcements and market attention, the UK Information Commissioner's Office (ICO) published a Tech Futures report on agentic AI. In doing so, it became the first data protection regulator to tackle the topic. The report does not constitute formal ICO guidance but does provide important insight to the regulator's view on data protection implications, risks and how organisations may be able exploit the opportunities the technology offers. The report delivers on the action set out in the ICO's AI and biometrics strategy to engage with industry to assess the data protection implications of agentic AI. It is intended to support the ICO's ambition to encourage the responsible development and use of agentic AI.

This blog takes an initial look at the key messages that can be drawn from the ICO's report and what organisations can learn at this stage of the regulator's policy thinking.

The ICO's report is to be welcomed in its assessment of evidence related to advancement, benefits and risk proliferation. Its nuanced approach provides a range of options as to how the technology may develop and be deployed. The report can therefore play a useful role in assisting organisations with initial risk assessments and planning for deployment.

The ICO has gathered significant evidence to inform the report and has transparently set out the methodology used and resources that can be considered alongside the report.

Definitions

Terms such as agents and agentic AI are often used interchangeably and the ICO helpfully provides definitions to enable a common language for our discussions about implications of agentic AI in the data protection community.

The ICO explains that an agent is *"software or a system that can carry out processes or tasks with varying levels of sophistication and automation."* It then explains that *"when large language models (LLMs) or foundation models are integrated ('scaffolded') with other tools, including databases, memory, computer operating systems and ways of interacting with the world, they create what industry is agentic AI."*

The ICO also notes that because agentic AI systems build on LLMs, some of the negative characteristic features of LLMs (such as hallucinations and bias) may be present.

Agentic AI can take different forms, perhaps as a standalone agent or, when several agents are, combined, as a 'multi-agent system'.

Likely evolution of agentic AI, capabilities and use cases

Four scenarios for the evolution of agentic AI are set out and explained in the ICO report:

1. Scarce, simple agents (low adoption, low agentic capability)

2. Just good enough to be everywhere (high adoption, low agentic capability)

3. Agents in waiting (low adoption, high agentic capability)

4. Ubiquitous agents (high adoption, high agentic capability)

It is important to understand the new capabilities that agentic AI may offer.

The report highlights perception (i.e. working with a wide range of inputs), planning or reasoning-like actions (e.g. generating plans, dividing tasks, error checking), action (e.g. accessing tools, interacting with people or AI agents, running code), and learning and memory (i.e. adaptive decision making, correcting errors in future plans, learning preferences and from feedback) as capabilities likely to be demonstrated by agentic AI systems to some extent. The report also indicates that capabilities are being assessed by researchers based on autonomy, efficacy, goal complexity, generality and under-specification. The ICO's report therefore focuses on how agents can autonomously pursue goals, adapt to new situations and contexts, and an exhibit some reasoning-like capacities.

Potential use cases covered in the report include research, coding, and planning, organising and executing transactions.   Use in agentic commerce, workplace applications, government services, automated cybersecurity applications, integrated personal assistants and the medical sector are also covered in the report, indicating a wide range of potential deployments.

It is also important to note that the ICO's assessment of the stakeholder evidence in the report indicates that the rate of improvement in LLM capabilities may slow or even stop in the short to medium term. The graph of agentic technology evolution may not be a linear one.

Looking further ahead, amongst other things, the ICO sees evidence that the following technical developments could emerge - truly multimodal agents, increasing agent autonomy and agent-to-agent communication and agentic AI embedded into a wider range of software and devices.

Key data protection implications

Accountability and governance

A key message from the ICO is on accountability- organisations must continue to take responsibility for AI in the context of data protection:

> *"AI agency does not mean the removal of human, and therefore*

> *organisational, responsibility for data processing. Organisations must be clear on the expectations that still apply under data protection legislation."*

The ICO notes that currently, and for the foreseeable future, organisations can control factors such as the actions the agent is authorised to take and the information the agent can access. An important learning point for organisations planning agentic AI governance is to prioritise the effective risk assessment of these elements and ensure that relevant controls are in place.

On governance, the ICO highlights the importance of flexible and adaptable governance to move with changes in how agentic AI systems may operate. Whilst not a formal endorsement, the ICO highlights the relevance of the Safer Agentic AI Foundations, from the Agentic AI Safety Community of Practice. The ICO also indicates that organisations may need a separate, standalone monitoring system.

The report's section on accountability is relatively short at half a page, and it will be helpful for organisations if greater coverage is given to this topic in future ICO publications. Such further output could include information on how existing AI governance models will need to evolve, including existing AI standards and risk management frameworks such as those in use from NIST and ISO. It will also be relevant to address how to scale governance, and the balance between centralisation and decentralisation. Organisations will also need to address the risks of shadow AI, which could proliferate further with use of unauthorised AI agents, and how agents are managed and ultimately removed from use when no longer needed.

Novel risks

Data protection issues that may arise in the context of AI more generally, and particularly generative AI, can also be seen (perhaps even to a greater extent) in the context of agentic AI. Novel agentic AI data protection risks are also highlighted in the report, including:

- issues in relation to determining controller and processor responsibilities through the agentic AI supply chain;

rapid automation of increasingly complex tasks resulting in a larger amount of automated decision-making;

purposes for agentic processing of personal information being set too broadly so as to allow for open-ended tasks and general-purpose agents;

agentic AI systems processing personal information beyond that which is necessary to achieve instructions or aims;

potential unintended use or inference of special category data;

increased complexity impacting transparency and the ease with which people can exercise their information rights;

new threats to cyber security resulting from, for example, the connected and autonomous nature of agentic AI;

and the concentration of personal information to facilitate personal assistant agents.

The section of the report on automated decision making (ADM) sets out some general impacts that must be considered but is otherwise surprisingly short given the challenges that agentic AI may pose in this area. This appears to be because the ICO will set out its thinking on ADM and AI in more detail in the forthcoming code of practice.

It will be important for the ICO to explore issues of human intervention in more detail in future publications, including the role of alternatives to human in the loop solutions, such as human on the loop.

The Tech Dispatch Report of the European Data Protection Supervisor is also helpful reading in this area.

Role of agentic AI in automating data protection compliance

Lastly, the report sets out how agentic AI could pose challenges for DPOs in maintaining oversight, but also how agentic AI could assist the process of data protection compliance itself. The report sets out the idea of 'DPO agents' i.e. systems that are integrated into data protection teams to scale and augment the role of human staff. The report also notes how privacy and personal information management agents could help people manage their own privacy settings and controls.

The ICO also calls for innovation in methods for the practical evaluation of the compliance of agentic AI systems with data protection legislation.

Next steps

The ICO has committed to publish a new statutory code of practice on AI and data protection in 2026 and we can expect a consultation process in the coming months.   The code is expected to have a specific focus on automated decision making, which will be particularly relevant to the implementation of agentic AI.

We can also expect collaboration internationally with other DP regulators and with UK regulators via the Digital Regulation Cooperation Forum , workshops with stakeholders, and advice via the ICO's innovation service and regulatory sandbox.

Related capabilities

Artificial intelligence

Data privacy and data protection

SUBSCRIBE

Interested in this content?

Sign up to receive alerts from the A&O Shearman on data blog.

SIGN UP →

Register or update your preferences