Pritchetts

Welcome to our Autumn 2026 Newsletter!

In This Issue

- The new Information Commission Secures Data Protection Changes from Ten Major AI Developers
- The ICO Turns Its Attention to "Agentic AI"
- Swamped by DSARs? Why Access Requests Are Getting Harder to Handle
- UK Direct-Marketing Law Has Changed: Is Your Organisation Ready?
- A New Approved Information-Sharing Code for Public Services in Wales
- Cyber Resilience Remains a Priority
- Governance Remains at the Heart of Compliance
- Free Training from the ICO: Data Protection Essentials
- Pritchetts Law Recognised in Chambers UK 2027 and The Legal 500 UK 2027

Quick Links

More About Us

Our Services

Testimonials

Our Published Articles

Artificial Intelligence

Data Protection & Privacy

Contact Us

The frost on the car this week suggests this might be more of a winter newsletter. As we approach the end of another busy year, organisations continue to face an increasingly complex compliance landscape. Artificial intelligence remains at the top of many boardroom agendas, cyber resilience continues to attract regulatory attention, and organisations are under growing pressure to demonstrate effective governance around the technologies they use.

Many of the developments covered in this edition build directly on themes from our Summer 2026 Newsletter. In particular, AI governance, cyber resilience and accountability remain key areas of focus for regulators both in the UK and beyond.

We've rounded up some of the most important developments from the last few months, together with some practical considerations for organisations.

As always, if any of these issues affect your organisation, or you would simply like to discuss how these developments might apply to your business, please do not hesitate to get in touch.



The new Information Commission Secures Data Protection Changes from Ten Major AI Developers

As Artificial Intelligence evolves, regulators are increasingly focused on ensuring innovation is accompanied by appropriate safeguards.

For the pub quiz: Following the Data (Use and Access) Act 2025 (**DUAA**), the Information Commissioner's Office, was replaced by the Information Commission on 30 September 2026 and continues to be known as the **ICO**.

The ICO announced on 8 October 2026, that ten leading AI foundation model developers had either made, or committed to make, changes following engagement with the ICO. These commitments were secured from some of the world's most influential AI developers: Microsoft, OpenAI, Google, Meta, Amazon, Anthropic, Apple, Cohere, DeepSeek and Stability AI.

The commitments include clearer transparency information, stronger mechanisms for people to exercise their rights and tougher assessments of safeguards, and the ICO says it is monitoring progress against those commitments.

What makes this development particularly significant is that the ICO is no longer talking solely about hypothetical risks – it has made enquiries with OpenAI, Anthropic, Meta and the UK AI Security Institute following reports that, in recent testing, certain AI agents bypassed protections, used unauthorised communication channels and accessed external systems.

For organisations using AI tools, whether through Microsoft Copilot, Anthropic's Claude, ChatGPT, or their own internal AI solutions, this is a timely reminder that governance should be keeping pace with adoption.

What should organisations be asking?

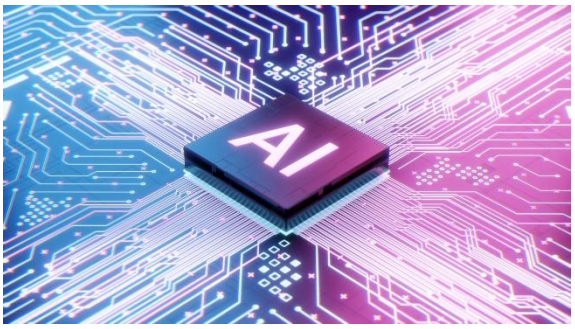
- Do we have an AI policy and governance framework?
- Do we know where AI is being used throughout the business, and what is it being used for?
- Have we assessed privacy and confidentiality risks for those uses?
- Do staff understand what information should not be entered into AI systems?
- Have suppliers' own use of AI been appropriately assessed?

Building on our Summer 2026 Newsletter, we discussed how AI regulation is moving from theory to enforcement and why governance must evolve as AI tools develop. Recent ICO activity demonstrates that regulators are now moving beyond guidance and increasingly influencing market practice.

How we can help

We support organisations with AI governance frameworks, AI policies, AI risk assessments, AI-related DPIAs, supplier due diligence and staff training. Find out more about our artificial intelligence services.

The ICO Turns Its Attention to "Agentic AI"



Just as many organisations are becoming comfortable with generative AI, regulators are already looking at the next phase of development.

On 8th October, the ICO launched a call for evidence on "agentic AI" systems. These systems are designed to take actions, make decisions and perform tasks with reduced human intervention. The call for evidence closed on 20 November 2026 and covered data security, transparency, accountability, automated decision-making, fairness and purpose limitation, and lawfulness of processing. The consultation will inform the ICO's future guidance and its forthcoming statutory code of practice on AI and automated decision-making.

Examples of agentic AI are already beginning to appear within business environments through AI assistants, workflow automation tools and AI-powered business processes.

Whilst these technologies create exciting opportunities, they also raise important questions about oversight and governance.

Practical considerations

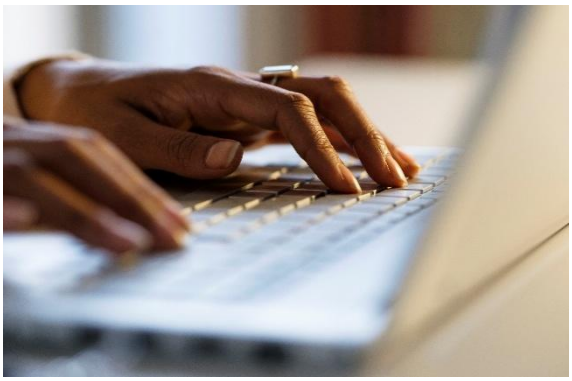
Organisations considering the use of AI agents may wish to consider:

- Who remains accountable for decisions taken by AI systems?
- What oversight mechanisms are in place?
- How are risks assessed before deployment?
- What safeguards exist if an AI system behaves unexpectedly?

Many organisations have now adopted an AI policy. Far fewer have considered governance arrangements for AI systems capable of acting with significantly greater autonomy.

How we can help

We can help organisations assess AI governance arrangements, review AI deployments and implement practical controls that balance innovation with compliance.



Swamped by DSARs? Why Access Requests Are Getting Harder to Handle

Data subject access requests (**DSARs**) are among the most common individual rights requests organisations receive. They can quickly become resource-intensive, particularly where information is spread across email, messaging platforms, shared drives, archives and third-party systems. They are also often stressful, arriving alongside litigation or staff disciplinary processes. These are not fun for anyone to deal with, in particular if you've got a day job to do.

A compliant response involves more than collecting documents. Organisations may need to verify identity, clarify scope, carry out reasonable and proportionate searches, deal with duplicates and third-party information, consider legal professional privilege and other exemptions, and disclose securely, all while justifying and recording their decisions along the way. A clear, repeatable and documented process remains the best way to respond consistently and defend decisions if challenged.

The ICO has recently published guidance on dealing with AI supported DSARs. While they acknowledge that AI is leading to more frequent and more detailed DSARs, they are very clear that the rules on DSAR responses are no different. So, some welcome regulator sympathy, and a useful summary of the general DSAR rules, but no specific change in their requirements.

Our article explains why DSARs and other rights requests are getting harder and how organisations should prepare. Read our recent article: Swamped by DSARs?

If you would like help with DSAR handling, search approaches or response procedures, please contact us.

UK Direct-Marketing Law Has Changed: Is Your Organisation Ready?



Direct marketing is one of the areas that attracts the most ICO attention, and enforcement. The Privacy and Electronic Communications Regulations 2003 (**PECR**) cover direct marketing by email, text, social media, direct messages and calls, as well as cookies and other tracking technologies. Since 5 February 2026, breaches of the marketing and cookie rules under PECR, can attract fines of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher, for conduct from that date. This is a substantial increase, compared with the £500,000 limit previously in place.

Direct marketing is also now in the UK GDPR as a statutory example of processing that may be carried out for a legitimate interest. This is not a free pass: you must still pass the legitimate interests test (recording your assessment). PECR consent requirements also still apply where you are sending electronic direct marketing or using cookies (other than those covered by the new, narrow exemptions for certain lower risk cookies, such as some statistical and appearance cookies).

Our article also reviews nine ICO marketing fines published between December 2025 and November 2026, ranging from £100,000 to £300,000 (all for breaches before the higher limit applied), explains the ICO's new AdTech 3.0 report on AI-driven advertising and sets out practical steps to take. Direct Marketing in 2026: New ICO Guidance, Bigger Fines and AI-Driven Advertising.

Practical questions

- Do we know which channels we use, and what rules apply to each?
- Do we need to treat marketing to consumers, sole traders or companies differently? If so, which rules apply to each?
- Is our consent wording clear (not pre-ticked) and documented? Where we rely on the soft opt-in (including the new charity version), did we offer an opt-out when we collected details, and do we include one in every message?
- Are we sending direct marketing on the basis of legitimate interests? If so, do we need to complete (or update) a legitimate interests assessment?
- Do any of our "service messages" include promotion? Do we need to handle service messages differently to marketing messages?
- Are opt-outs and objections acted on promptly, and are marketing calls screened against the TPS/CTPS (the telephone preference registers)?
- Do we have a data protection complaints process (a legal requirement since 19 June 2026) that covers complaints about our use of personal data in marketing?
- Do we know where our marketing data comes from, including lead generators and call centres? Do we need to complete due diligence, and check our contracts?
- If we use AI-enabled advertising tools, do we know what personal data they use, who is responsible for what, and whether we need a DPIA?
- Have our privacy notices, cookie banners and any AI-driven profiling been checked against the ICO's latest guidance?

If you would like help reviewing your marketing practices, consent wording, legitimate interests assessments, DPIAs, AdTech and AI-driven advertising tools or cookies, please contact us.



A New Approved Information-Sharing Code for Public Services in Wales

Information sharing continues to present challenges for many businesses and professional services firms.

In September, the ICO approved the WASPI (Wales Accord on the Sharing of Personal Information) UK GDPR Code of Conduct for Information Sharing Protocols, which was published on 28 September 2026. The Code has been developed to support organisations sharing personal information to deliver health, education, social care, safeguarding and other public services in Wales. The Code's monitoring body is still awaiting ICO accreditation.

Many organisations recognise the importance of protecting personal data but are often less confident when it comes to determining when information can be shared lawfully.

The new Code seeks to provide a structured and consistent approach to information sharing arrangements.

Why this matters

Although the Code is specific to Wales, similar questions arise wherever organisations work closely with:

- Professional advisers
- Contractors and suppliers
- Strategic partners
- Group companies
- Educational institutions
- Public bodies

A failure to share information when it is appropriate can create operational difficulties, whilst sharing information without sufficient safeguards can create legal risk.

How we can help

We regularly assist clients with information-sharing agreements, governance frameworks, DPIAs and wider compliance reviews.

Cyber Resilience Remains a Priority



Readers of our Summer 2026 Newsletter may remember our discussion of lessons from recent cyber security enforcement action and what the proposed Cyber Security and Resilience Bill could mean for businesses.

These themes continue to be relevant as regulators and policymakers maintain their focus on cyber resilience.

On 1 October, the Information Commission (ICO) joined the National Cyber Resilience Centre Group's National Ambassador Programme, reinforcing its commitment to improving cyber resilience and helping organisations strengthen their security practices. The ICO says the partnership will help connect small and medium-sized businesses with free and affordable support available through police-led Cyber Resilience Centres.

The Cyber Security and Resilience (Network and Information Systems) Bill, which would reform the Network and Information Systems Regulations 2018, is now at its final parliamentary stages (the Commons is due to consider the Lords amendments today). It is not yet law. It would extend the existing regime, including to data centres and certain IT service providers, but the regime does not cover the whole economy. See more at the UK Parliament: Bill page.

The National Cyber Security Centre offers a free resource to help organisations rehearse their response to cyber attacks.

For organisations of all sizes, the message remains clear: cyber security is no longer solely an IT issue. It is a governance issue.

Questions organisations should ask

- Do we have a documented incident response plan?
- Has it been tested recently?
- Are employees receiving regular training?
- Are key suppliers being appropriately assessed?
- Is senior management receiving adequate information about cyber risks?

Building on our Summer 2026 Newsletter, this development reinforces many of the lessons we highlighted there from recent cyber security enforcement action.

How we can help

We support organisations with the legal and data protection aspects of cyber governance, incident response planning, tabletop exercises, staff training and personal data breach response, including regulatory notification.



Governance Remains at the Heart of Compliance

Although the headlines often focus on AI, cyber attacks or enforcement action, a common theme continues to emerge across all areas of regulatory activity.

Organisations are increasingly expected not only to comply with legal requirements but also to demonstrate how compliance is achieved.

Whether considering AI, cyber security, data protection or marketing practices, regulators continue to focus on:

- Accountability
- Training
- Policies and procedures
- Risk assessments
- Record keeping
- Senior management oversight

Organisations that can demonstrate robust governance arrangements are generally better placed to respond to regulatory scrutiny, security incidents and changing legal requirements.

A Useful Question

If a regulator asked your organisation tomorrow how you govern AI, cyber security and personal data, could you confidently demonstrate your approach?

If not, it may be time for a governance review.

How we can help

Our team provides a range of services including:

- Data protection compliance audits and wider governance reviews
- LOCS:23 consultancy support (for the legal sector)
- Policy reviews
- DPIAs
- Contract and data processing agreement reviews
- Data protection training
- AI governance support

Free Training from the ICO: Data Protection Essentials



In August 2026, the ICO launched Data Protection Essentials, a free online course with a built-in self-assessment, aimed at sole traders and smaller organisations. Learners work through 13 short modules, each taking roughly 10 to 15 minutes, at a time that suits them. The examples are tailored to a number of sectors, including education and childcare, health and social care, professional services, retail and property. Everyone who finishes the course receives a digital certificate, and an organisation that completes the self-assessment can ask to be named on the ICO's public register.

Separately, the ICO has opened up the internal training modules it gives its own staff on data protection law and information governance, so that other organisations can reuse them in their own training. The topics include what counts as personal data, special category data, the data protection principles, individual rights and exemptions, so you can pick the ones that are relevant and add them to your existing training. The ICO's training and resources page also has a free checklist that gives practical suggestions for improving how you train your own staff.

These are a useful starting point, particularly for organisations without in-house data protection expertise. But they are general materials, designed for smaller, lower-risk organisations, and completing them does not of itself demonstrate compliance. Organisations with higher-risk processing, regulated clients, or teams working with AI tools, DSARs and marketing data will usually need more.

Questions organisations should ask

- Have all staff, including new joiners, received data protection training in the last 12 months?
- Is our training tailored to people's roles and the personal data they handle?
- Does it cover AI tools, DSARs, direct marketing, and spotting and reporting personal data breaches?
- Do we keep a record of who has been trained, and when?

How we can help

Our bespoke training is built around your organisation: your sector, your systems, your risks and the people being trained, from front-line staff to senior management. We can cover the ICO's essentials and go further into AI use, DSARs, direct marketing, data and cyber security risks and breach response.

If you would like to discuss our off-the-shelf or bespoke data protection training services, please get in touch.

Pritchetts Law Recognised in Chambers UK 2027 and The Legal 500 UK 2027

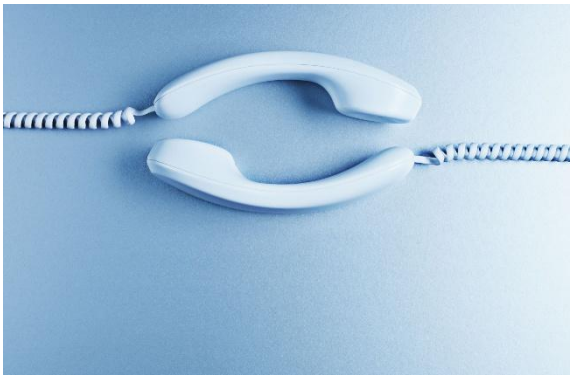
We're delighted to share that Pritchetts Law has once again been recognised and ranked in the latest editions of two of the best-known legal directories. We're ranked nationally in Chambers UK 2027 for Data Protection & Information Law and in The Legal 500 UK 2027 for IT and Telecoms in the South-West, and in its national rankings for data protection, privacy and cybersecurity.

Both directories base their rankings on independent research, including confidential feedback from clients and peers. We are very grateful to everyone who took the time to share their experience with the researchers.

Our article gives more detail on the rankings and what they mean for our clients. Pritchetts Law Once Again Ranked Among the Top UK Law Firms. We are really proud that our boutique specialist firm is rated for the quality of advice we deliver and ranked alongside some of the largest law firms in the market.

If you would like to talk about data protection, AI governance or technology contracts, please get in touch.

We'd Love to Hear From You



We're always happy to arrange a call and discuss what's happening in your organisation, whether that's implementing AI, responding to a data breach, managing a DSAR, reviewing your contracts, and governance arrangements or navigating new regulatory developments.

If any of the issues discussed in this newsletter are relevant to your organisation, please do get in touch for an informal, no-obligation conversation.

We look forward to hearing from you.

This newsletter is for general information only and does not constitute legal advice. Specific advice should be taken before acting on any of the issues covered.

Pritchetts Law LLP | info@pritchettslaw.com | +44 (0)117 307 0266 | pritchettslaw.com

See what's happening on our social sites:

