Pritchetts

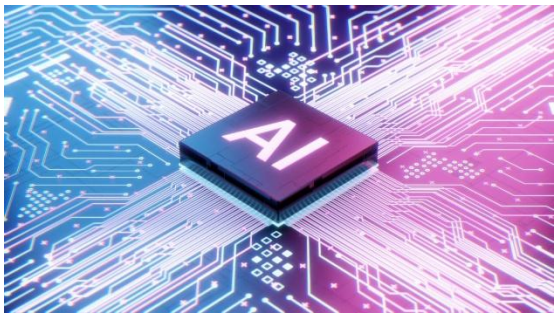
Welcome to the Summer 2026 issue of our Data Protection Newsletter!

In This Issue

AI Regulation Moves from Theory to Enforcement
UK Data Law Reform – Complaints Handling Deadline Is Now Passed
Cyber Enforcement Escalates – Governance Failures Are Costly
New UK Cyber Security Bill – Expanding Scope and Accountability
AI Continues to Evolve – Governance Must Evolve With It
Key Takeaways

Quick Links

More About Us
Our Services
Testimonials
Our Published Articles
Artifical Intelligence
Data Protection & Privacy
Contact Us



AI Regulation Moves from Theory to Enforcement

Artificial intelligence regulation is moving from policy into implementation, with both UK and EU frameworks becoming increasingly operational.

In April 2026, the UK introduced the **Data Protection Act 2018 (Code of Practice on AI and Automated Decision-Making) Regulations 2026** , requiring the ICO to produce a formal code of practice covering the development and deployment of AI systems.

At the same time, the ICO has continued to expand its guidance on AI governance, with a clear emphasis on **fairness, explainability and accountability in automated decision-making** . [ico.org.uk]

Across Europe, the **EU AI Act** is approaching a major implementation milestone. While some deadlines may shift, **its obligations apply on a phased basis, with further requirements expected to become applicable around the August 2026 implementation window** , including obligations relevant to higher-risk systems, transparency, documentation and governance requirements. [ico.org.uk]

This is no longer a future compliance exercise. It is a current governance issue.

What this means in practice:

- Documentation, auditability and appropriate human oversight are increasingly regulatory expectations - not merely optional “good practice”, particularly where AI affects individuals or involves personal data.
- Organisations must identify where AI is used, particularly where it is used in decision-making (beyond obvious use cases).
- UK organisations selling into the EU, and EU organisations operating in the UK, may need to operate dual compliance models to manage overlapping UK data protection and EU AI Act compliance requirements.

How we can help:
We are advising organisations on:

- AI governance frameworks aligned to UK GDPR and EU AI Act requirements
- Data protection impact assessments (DPIAs)
- AI risk assessments
- Drafting internal policies and accountability structures
- Preparing for regulatory scrutiny of AI usage, and automated decision-making

---

UK Data Law Reform – including a Complaints Handling Deadline Now Passed



The **Data (Use and Access) Act 2025 (DUAA) reforms** have continued to be phased in. The latest change has been **the requirement** to have a mandatory data protection complaints process in place by **19 June 2026** . [ico.org.uk]

What does this mean for you?

- Your privacy notices should be updated to explain your data protection complaints process.
- You must have a process in the background to handle those complaints efficiently and to keep individuals informed.
- Staff should be made aware, and trained on the new requirements, and your process.

- You should maintain records of complaints, acknowledgements, investigations, outcomes and any remedial action, so that you can evidence compliance if challenged.

Organisations should also continue considering the impact of other key DUAA changes:

- I **ncreased fines for PECR breaches** . Since 5 February 2026, fines for activities falling within the PECR rules, such as electronic direct marketing, and cookie and tracking technology compliance, are now subject to the same limit as other data protection breaches under the UK GDPR – so up to **£17.5 million or 4% of total worldwide annual turnover** for the previous financial year (whichever is higher). These marketing fines were previously capped at £500,000, so the change materially increases enforcement risk for electronic marketing, cookies and tracking technology compliance.
- **Cookies, pixels and tracking technologies remain a live compliance risk** . The ICO's updated guidance is a reminder that compliance is not just about having a cookie banner. Organisations should understand what cookies, pixels, scripts, tags and similar "storage and access technologies" are active on their websites, apps and communications, whether consent is required, whether any exception applies, and whether users are given clear and effective choices.
- **Legitimate interests.** Certain processing activities are now expressly recognised as potentially necessary for an organisation's legitimate interests, including: direct marketing, intra-group transfers for internal administrative purposes, and network and information security. This may simplify part of the legitimate interests analysis, but organisations still need to assess purpose, necessity and balancing against individuals' rights and interests.
- **Charities** have greater scope to rely on legitimate interests for some direct marketing, but PECR consent rules and opt-out requirements still need to be considered, particularly for electronic marketing.
- **Relaxation of the purpose limitation** . DUAA gives organisations greater flexibility for compatible processing for research, statistical, and scientific purposes, but this remains subject to applicable safeguards, transparency requirements and the wider UK GDPR framework.
- DUAA introduced certain "**recognised legitimate interests** ", such as specified processing connected with public security, emergencies, crime prevention and safeguarding. Where the relevant conditions are met, the usual balancing test is not required, but organisations must still confirm that the processing falls within scope and comply with the wider UK GDPR principles. In those cases, the legal basis analysis should usually be simpler, but it should still be documented.
- **Changes to automated decision-making prohibition** . Particularly where special category data is not involved, DUAA introduced a more **permissive framework for solely automated significant decision-making** , which removes the total prohibition on using personal data to make significant decisions about individuals without meaningful human involvement. Examples may include decisions about recruitment, lending, benefits or eligibility for services etc. Organisations must, however, still assess whether the decision is in scope, identify an appropriate lawful basis, implement safeguards, provide meaningful information to individuals and allow routes for challenge or human review where required.
- **Subject access request handling** has been clarified in some areas, including the requirement to carry out reasonable and proportionate searches and the ability to pause response time while awaiting clarification in appropriate cases.

Children's data and age assurance are also moving up the enforcement agenda.

Organisations operating online services that may be accessed by children should reassess whether their **age assurance**, transparency, profiling, default settings and data minimisation measures remain appropriate. Self-declaration alone is unlikely to be sufficient for higher-risk services.

How we can help:

We are continuing to support clients with:

- Handling subject access requests and other rights requests.
- Updates to privacy notices, and implementation of complaints handling frameworks (aligned to ICO expectations).
- Reviewing cookie banners, consent management platforms, marketing compliance, tracking technologies and website/app privacy compliance.
- Reviewing AI and automated decision-making processes for compliance.
- Children's data risk assessments, age assurance reviews and alignment with data protection and online safety expectations.
- Updates to policies and procedures, to support accountability and to implement DUAA changes.
- Practical compliance audits and gap analysis projects focused on evidencing accountability.

If your complaints process, privacy notices or staff guidance have not yet been updated, this should now be treated as a priority compliance action.

If you would like to know more about the legal requirements for handling data in your organisation, get in touch with Pritchetts.



Cyber Enforcement Escalates – Governance Failures Are Costly

Recent ICO enforcement activity shows a continued focus on **basic governance and cyber resilience failures** .

In May 2026, the ICO fined South Staffordshire Plc **£963,900 following a cyber attack affecting over 630,000 individuals** , where attackers remained undetected for almost two years.

The regulator identified failings in:

- Monitoring and detection
- Access controls and vulnerability management
- Incident response preparedness and broader security governance.

Earlier enforcement trends reinforce the same message:

- £15m in fines issued in late 2025 for cyber-related breaches linked to inadequate security controls [ico.org.uk][ico.org.uk]
- Ongoing enforcement around children's data, marketing, and lawful basis failures [ico.org.uk][ico.org.uk]

The consistent theme is clear:
Cyber risk is being regulated as a governance failure - not just a technical issue.

What this means in practice:

- Boards and senior leadership teams are increasingly expected to understand and oversee cyber, data security and data governance risk.
- "We didn't know" is no longer a credible position - a lack of visibility over cyber risk is increasingly difficult to defend.
- Evidence of proactive risk management is critical.

How we can help:
We work with organisations to:

- Align security controls with UK GDPR expectations
- Design defensible incident response and **personal data breach handling** frameworks
- Stress-test accountability before regulatory scrutiny – getting your **policies, procedures** and **training needs analysis/ training programmes** up to scratch

New UK Cyber Security Bill – Expanding Scope and Accountability



At the time of writing, the UK government's **Cyber Security and Resilience Bill** is progressing through Parliament and represents the most **significant reform of cyber regulation** since the introduction of the Network and Information Systems (NIS) regime. The proposals are intended to strengthen the UK's cyber resilience by **expanding the organisations that fall within scope** , increasing reporting obligations and enhancing regulatory oversight.

The Bill is expected to introduce:

- The inclusion of medium and large managed service providers that meet the definition of "relevant managed service provider" (i.e. unlikely to apply to micro and small MSPs unless they are providing essential services), certain data centres and other designated critical suppliers within or closer to the regulatory framework.
- More stringent incident reporting requirements, including a light-touch initial notification within 24 hours and a fuller report within 72 hours for relevant incidents.
- Enhanced regulatory powers and enforcement mechanisms.
- Increased focus on supply chain resilience and systemic cyber risk.

Ransomware and supply chain compromise remain central cyber resilience risks.

Organisations should understand which suppliers support critical operations, what security commitments are contractually required, and whether incident response plans cover supplier-led disruption as well as direct attacks.

What all this means in practice:

- Organisations that have not previously been subject to cyber-specific regulation may now need to assess whether they fall within scope – and will carry regulatory obligations, not just contractual obligations.
- Supplier and outsourcing arrangements may require greater scrutiny to ensure cyber and resilience risks are appropriately addressed.
- Incident response processes will need to support faster reporting and escalation obligations.
- For serious breaches, proposed fines may reach the higher of £17 million or 4% of global turnover (noting that detailed rules about how to calculate turnover and enforcement practice are yet to come).
- Senior leadership teams should ensure that cyber risk and resilience are appropriately considered within broader governance and risk management frameworks.

How we can help
We are advising organisations on:

- Assessing whether the new regulatory requirements apply to their organisation.
- Reviewing supplier, outsourcing and technology contracts, incident response playbooks and escalation and breach processes, to ensure cyber resilience obligations are addressed, data protection risks are properly allocated, and relevant legal and regulatory risks are managed.
- Understanding incident reporting obligations and associated compliance requirements.
- Developing governance, accountability and risk management frameworks that support regulatory compliance.
- Supporting organisations in demonstrating compliance to regulators through appropriate policies, procedures and documentation.



AI Continues to Evolve - Governance Must Evolve With It

Artificial intelligence is **developing at an extraordinary pace** . While many organisations are now familiar with tools such as Microsoft Copilot, ChatGPT and other generative AI platforms, the challenge is that the **technology rarely stands still** .

New **AI tools emerge regularly** , existing products continually gain **new capabilities** , and integrations with other systems create **new opportunities and risks** . These may not have existed when a tool was first approved for use.

As a result, organisations often find that their **understanding** of an AI system quickly becomes **outdated** . A tool initially introduced to assist with drafting documents may later analyse data, generate code, automate workflows, interact with third-party systems **or influence decision-making** . Employees may also **develop new use cases** that were **never anticipated** during procurement or deployment.

Meanwhile, AI providers continue to release new models, expand functionality and deepen integrations across email, HR, CRM, project management and business intelligence platforms. This means many **organisations may be using AI in more areas** - and processing more data, or creating wider data access and disclosure risks, than they originally assessed or intended.

Examples of how AI use can evolve include:

- The organisation embraces AI agents and they are increasingly being used to take actions, interact with systems or make recommendations on behalf of users. Organisations need clearer controls over authority, oversight, audit trails, data access and escalation routes.

- A drafting tool becoming a tool for contract analysis, obligation extraction or decision support.
- An AI tool originally approved for limited internal use being connected to email, Teams/chat, SharePoint, CRM, HR or finance systems – potentially exposing significantly more data to the AI tool.
- A familiar platform introducing new models, sub-processors, data flows or overseas processing arrangements that were not considered in the original review.
- Employees using approved AI tools for unapproved "shadow" purposes, including uploading client, employee or confidential business information.
- A customer service chatbot moving from answering questions to prioritising complaints, recommending refunds or influencing escalation decisions.
- An HR assistant progressing from administrative support to candidate screening, absence management or performance review preparation.
- A business intelligence or fraud tool beginning to generate risk scores, predictions or behavioural insights about individuals or customers.

Evolving AI and Agentic AI creates a governance challenge .

Traditional compliance approaches often assume that systems remain relatively static once implemented. AI is different: functionality, data flows and risk profiles can change over time, sometimes **without organisations fully recognising the implications.**

What this means in practice:

- AI **risk assessments** should not be treated as a one-off exercise;
- **Governance frameworks should include periodic reviews of AI tools and their capabilities;**
- Organisations should monitor how employees are actually using AI rather than relying solely on intended use cases;
- New **integrations, updates** and **functionality** should trigger reassessment of legal, compliance and information governance risks – including whether existing DPIAs remain adequate.

AI governance is about managing an evolving technology landscape in which capabilities, use cases and risks can change rapidly.

How we can help:

- **AI governance frameworks and accountability structures.**
- Reviews of **existing AI deployments** and emerging use cases.
- Assess whether AI tools are being used merely for assistance, or whether they are **beginning to make or influence operational decisions** .
- DPIAs and AI risk assessments of **new tools, integrations** and **functionality** .
- **Policies and procedures designed to manage evolving AI risks.**
- Ongoing **compliance and governance programmes** for AI use.

Key Takeaways – What organisations should be prioritising



Across all sectors, we are seeing a convergence of three pressures:

1. **AI governance is moving from concept to enforcement.**
2. **AI tools are evolving faster than many organisations' governance and compliance processes.**
3. **AI, data protection and cyber security are increasingly being treated as a board-level accountability issues.**

The common thread is **governance maturity** .

Organisations that succeed are those who can:

- Evidence decisions
- Demonstrate accountability
- Operate repeatable, tested processes

If You Would Like to Discuss These Developments

If you would like to understand how any of these developments affect your organisation, we can help you prioritise the practical steps to take now — from support building a defensible data governance framework, AI governance and risk assessments, compliance with DUAA changes, to cyber resilience, supplier risk and incident response plans. Please contact us if you would like to arrange a free of charge and no-obligation discussion.

We would also love the opportunity to assist with your organisation's **data protection training programmes** – we offer both **tailored in-house training** or **off-the shelf data protection training** packages.

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.

See what ’s happening on our social sites:

