

Data, Privacy and Cyber Predictions 2026

Data protection complaints (and complaints about complaints) will increase

The Data (Use and Access) Act 2025 provides data subjects with a new statutory "right to complain". Once the relevant provisions are effective, controllers will need to ensure they have a complaints policy in place which meets the new requirements (including mandatory acknowledgement within 30 days). While many controllers will already have a complaints process in place, all will need to review these policies to ensure compliance with the new regime. This will ease the growing workload of the Information Commissioner's Office (ICO), particularly as data subjects will be formally required to raise a complaint with the relevant controller prior to pursuing a complaint with the ICO, but it is likely to have the opposite effect on controllers. This may be exacerbated by the recent significant increase in the use of generative AI by data subjects to submit complaints more quickly and in greater volume. If controllers are not prepared for the potential tidal wave of complaints, the mere failure of adequately handling complaints could result in further ICO investigations and liability beyond the subject of the original complaint.

Pseudonymisation: ambitious data use will require robust safeguards

As the sector seeks to unlock the value of its datasets for analytics and AI training, the tension between anonymisation and pseudonymisation is becoming ever more pressing. True anonymisation remains the gold standard but often strips away the richness that gives data its value. Pseudonymisation preserves that utility but keeps data within the scope of data protection law. The Court of Justice of the European Union's SRB decision brings welcome nuance, confirming that whether pseudonymised data counts as personal depends on the realistic means of re-identification available to the controller, not theoretical possibilities. This more contextual approach could open new space for innovation, provided businesses can show re-identification risks are genuinely low. Those in the sector that invest early in verifiable safeguards and governance frameworks will be best placed to harness data confidently and compliantly in the age of AI.

Agentic AI will intensify data protection risks

Agentic AI (systems made up of autonomous agents that are capable of independent interaction and decision making) poses heightened data protection risks. Although it brings notable benefits in terms of efficiency and innovation, representing another evolution beyond generative AI, it also introduces new challenges. Unlike some earlier AI systems, many typical agentic AI system use cases rely heavily on processing personal data, including special categories of personal data or other sensitive categories such as financial information. Although many organisations have so far managed to apply governance controls to the use of generative AI in the workplace, the reduced human oversight evident in agentic AI significantly increases the challenge of implementing the same controls. As a result, data protection risks are likely to intensify.

The integration of AI solutions will increase the adoption of privacy enhancing technologies

Over the next 12 months, we will see greater adoption of privacy enhancing technologies (PETs) and their closer integration with AI systems. For several years, PETs have been highlighted as having the potential to aid data protection compliance, in a variety of different contexts. In its 2023 guidance on PETs, the ICO specifically cited privacy by design and by default; data minimisation; security; and secure data sharing as capable of being supported by PETs. However, since then we have seen only intermittent PET adoption by organisations. In the coming year, PETs such as homomorphic encryption and federated learning will be used increasingly to train AI models.

Quantum computing will be the next frontier

As quantum technology develops, we expect cyber insurers to start considering the potential systemic risks associated with the post-quantum era. Developments in quantum technologies are advancing rapidly and will offer huge opportunities to improve our lives. However, quantum computing will also pose the next significant challenge to cybersecurity and organisations are being urged to take steps to prepare for this now. The National Cyber Security Centre has already published guidance on the timeline for the migration to post-quantum cryptography (PQC) which starts now by identifying information, systems and cryptography which is at risk and ends in 2035 with the complete migration to PQC for systems, services and products.

For further information or
enquiries, please contact:

Hans Allnutt
Partner
hallnutt@dacbeachcroft.com

Jade Kowalski
Partner
jkowalski@dacbeachcroft.com


Justin Tivey
Partner
jtivey@dacbeachcroft.com

Patrick Hill
Partner
phill@dacbeachcroft.com



Scan here to view our
full suite of predictions
for 2026.

insurance.dacbeachcroft.com
dacbeachcroft.com

 Connect with us:
DAC Beachcroft LLP

 Follow us: DACBeachcroft