DAC BEACHCROFT

Data, Privacy and Cyber
Predictions 2027



AI-generated DSARs will change complaint handling

A surge in AI-generated data subject access requests (DSARs) and data protection complaints is currently driving organisations to reconsider their approach to managing these requests. AI tools have made it easier than ever for data subjects to generate detailed complaints, DSARs and follow-up correspondence, often referred to as 'agentic flooding'. Organisations are increasingly facing lengthy and disproportionate submissions, large volumes of information to review and near-instantaneous data subject responses, some of which are speculative, unsupported or based on misunderstandings or misapplications of data protection law. As the administrative and financial burdens on organisations grow, they are likely to push back more readily. Rather than engaging with every assertion and request, organisations will concentrate on scoping and proportionality, make greater use of available exemptions and challenge unreasonable demands where appropriate. The result will be a shift from simply responding to complaints and DSARs as received towards actively managing and triaging them in order to seek resolution of the true underlying issue.

ICO regulatory enforcement set to increase

The Information Commissioner's Office (ICO) has historically been criticised for lacking teeth, particularly in its response to cyber security incidents and data breaches. That position now appears set to change. Major fines have been relatively rare, often appealed or reduced, and enforcement action has been limited compared with the volume of reported breaches. Since April 2022, the Netting-Off Agreement has allowed the ICO to retain fine income, subject to an annual £7.5 million cap, to meet specified enforcement and litigation costs. Meanwhile, its proposed settlement regime would offer substantial penalty reductions to organisations that admit infringements and resolve cases at an early stage. Taken together, these measures could reduce the financial and procedural burden of enforcement, potentially enabling the ICO to pursue more investigations through to formal regulatory outcomes. Each successful outcome may also strengthen the regulator's reputation and willingness to intervene. In addition, powers introduced by the Data (Use and Access) Act 2025 will enable the ICO to require organisations to commission forensic investigations and report the findings, potentially reducing the regulator's investigative burden, streamlining enforcement and bringing more security failings to light.

The UK's innovation-first AI approach faces growing pressure

The UK's pro-innovation approach to the regulation of AI will be challenged in response to industry and public concerns over the safety risks associated with the development of artificial general intelligence and superintelligent systems. Reported incidents of agentic AI systems executing unsanctioned actions and demonstrating deceptive behaviour have emphasised the risks associated with the development of increasingly advanced AI models. A Private Member's Bill, the Artificial Superintelligence Bill, was introduced into Parliament in September 2026. While unlikely to pass, the Bill's proposal to prohibit artificial superintelligence systems and introduce monitoring and control powers illustrates the growing political appetite for more prescriptive regulation of advanced AI. Further significant AI-related incidents, whether involving misinformation, cyber security, critical infrastructure, autonomous decision-making or widespread workplace disruption, will quickly shift public sentiment and political priorities. As AI becomes more deeply embedded across sectors, the UK Government may face mounting pressure to change its approach and consider introducing a legislative framework to ensure that AI is developed and used safely and responsibly.

The AI era forces a rethink of data retention

Data deletion and retention will rise to the top of the boardroom agenda as insurers seek to reduce risk, improve data governance and prepare for an AI-enabled future. For many in the data and privacy sector, historic approaches to retaining data are becoming increasingly difficult to justify. Growing volumes of legacy data increase cyber exposure, storage costs and regulatory risk, while also raising questions around compliance with data protection principles. At the same time, firms are looking to harness AI and advanced analytics, placing greater scrutiny on the quality, provenance and governance of the data they hold. We expect firms to move beyond policy reviews and launch more ambitious retention and deletion programmes. The challenge will be balancing legal, regulatory and business requirements to retain information against increasing pressure to justify why data is kept in the first place.

For further information or enquiries, please contact:

Hans Allnutt, UK
Partner
hallnutt@dacbeachcroft.com

Pilar Rodriguez Lopez, Spain
Partner
prodriguez@dacbeachcroft.com



Cyber risk in the supply chain will remain a board-level concern

Cyber risk in the supply chain will remain a board-level concern as firms become increasingly dependent on complex networks of technology providers, outsourced services and data partners. Recent years have demonstrated that organisations are often only as resilient as their weakest supplier. As the sector continues to adopt cloud services, AI solutions and digital platforms, the potential for operational disruption, cyber incidents and data breaches originating within the supply chain will continue to grow. We expect increased regulatory scrutiny of supplier oversight, contractual risk allocation and incident management arrangements. Firms will be expected not only to understand their critical dependencies, but also to demonstrate that appropriate governance, due diligence and ongoing monitoring processes are in place throughout the supply chain.

Critical infrastructure rules to become a cyber underwriting benchmark in Hong Kong

Codes of Practice implementing Hong Kong's Protection of Critical Infrastructures (Computer Systems) Ordinance will become an increasingly important benchmark for both regulatory scrutiny and insurers' assessment of cyber risk exposures. Regulators spent much of 2026 publishing a suite of guidance documents aimed at helping designated operators implement the new regime. Organisations continue to embed the new requirements and, although regulators do not publish a list of designated critical infrastructure (CI) operators, the legislation does not prohibit operators from disclosing that designation. Insurers writing risks that may be affected by a CI operator designation are well advised to seek proper disclosure at placement. The generic and sector-specific Codes of Practice are likely to become the benchmark against which regulators assess organisations' cybersecurity arrangements following incidents.

Privacy reform in Australia to drive investigations, claims and penalties

Privacy regulation in Australia is tightening, increasing regulatory and liability exposure for organisations handling personal information. The 2024 amendments to the Privacy Act strengthened the enforcement powers of the Office of the Australian Information Commissioner and introduced a statutory tort for serious invasions of privacy. Further privacy reforms are expected to introduce a requirement that data practices be fair and reasonable, along with additional rights for individuals. Businesses can expect greater scrutiny of how personal information is collected, used and disclosed, particularly where large volumes of customer data are involved. Insurers should anticipate regulatory investigations and civil penalty proceedings, as well as statutory tort and third-party claims arising from data governance failures. Organisations that review their privacy frameworks regularly will be better placed to manage the compliance, reputational and insurance risks.

Privacy enforcement will test cyber cover in Ecuador

Ecuadorian privacy claims will put cyber wordings under pressure in 2027, addressing whether policies will respond to regulatory investigations and corrective measures in the absence of a cybersecurity breach. The data protection regulator's first enforcement action in December 2025, resulting in six-figure fines against two national sports bodies for processing user information without valid consent, demonstrates that possible insurance exposure extends to unlawful processing. Insurers are expected to revisit investigation triggers, defence costs and losses arising from orders to stop processing or delete data. AI-assisted underwriting and overseas claims handling will add scrutiny of decision records and data-sharing arrangements. Whether the policy responds to the alleged privacy violation will be the central coverage question, with fines and remediation costs requiring separate consideration under both the policy wording and applicable law.

Ireland stays at the centre of European Big Tech regulation

As AI, data governance and digital regulation evolve, Ireland is expected to remain at the centre of Europe's most significant regulatory investigations and technology disputes. Ireland's Data Protection Commission (DPC) has imposed €4 billion in fines on major technology companies based in Ireland, underlining its central role in enforcing European data protection laws. Most recently, the DPC issued a €403 million fine to Google over its handling of location data. Many of those decisions remain subject to appeal, meaning only a small proportion of the headline fines (some €20 million) has so far been collected. Because many global technology companies maintain their European headquarters in Ireland, the DPC is likely to remain one of the continent's most influential regulators, exerting a significant impact on those companies' operations, with several major investigations continuing into 2027.



Cyber insurance enters the Swedish mainstream

Cyber insurance will become an increasingly standard component of corporate risk management in Sweden. As cyber attacks continue to grow in frequency and severity, insurers are responding with higher premiums, increased deductibles and tighter policy terms. Organisations seeking cover will need to demonstrate a higher level of cyber resilience. Basic safeguards such as incident response plans and staff training will become prerequisites for cover, not optional extras. In July 2026, Swedish organisations faced an average of 2,352 cyberattacks per week, a 36% increase since last year, making Sweden the most targeted country in the Nordics. Municipalities remain the prime target, followed by the finance sector and healthcare. This is coupled with a rise in cyber extortion against Swedish small businesses of 188% in 2026.

Scan here to view our full suite of predictions for 2027.

insurance.dacbeachcroft.com

dacbeachcroft.com

Connect with us:
DAC Beachcroft LLP

DAC Beachcroft publications are created on a general basis for information only and do not constitute legal or other professional advice. No liability is accepted to users or third parties for the use of the contents or any errors or inaccuracies therein. Professional advice should always be obtained before applying the information to particular circumstances. For further details please go to www.dacbeachcroft.com/en/gb/about/legal-notice. Please also read our DAC Beachcroft Group privacy policy at www.dacbeachcroft.com/en/gb/about/privacy-policy. By reading this publication you accept that you have read, understood and agree to the terms of this disclaimer. The copyright in this communication is retained by DAC Beachcroft. © DAC Beachcroft 2026. Prepared November 2026.