DATA, PRIVACY AND CYBER
PREDICTIONS 2025

DAC BEACHCROFT

For further information or enquiries, please contact:

Hans Allnutt
Partner
hallnutt@dacbeachcroft.com
+44 (0) 20 7894 6925

Jade Kowalski
Partner
jkowalski@dacbeachcroft.com
+44 (0) 20 7894 6744

Scan here to view our full suite of predictions for 2025.

1. Data processors will find themselves under increased scrutiny

Following the Information Commissioner's Office's (ICO) stated intention to issue the first fine to a processor for breach of its obligations under data protection law, processors will look to shift how they document their own compliance, including due diligence when appointing sub-processors in their supply chain. It will also result in many processors likely adopting a more robust position in contracts with controllers when negotiating liability caps for data breaches. Although the final penalty or enforcement notice has not been issued yet, the provisional decision has undoubtedly created a renewed focus and raised potential concerns for processors, reminding them of the importance of things like multi factor authentication. In the event that further fines are levied against processors in the coming year, the rationale behind these regulatory decisions will be awaited with great interest. Any fines issued to private sector or public sector controllers will provide additional understanding on whether the ICO will look to take a harsher line on processors who deliver software and services to the public sector only, or whether the ICO is adopting a wider remit of targeting processors across all sectors.

2. Approach to regulatory enforcement will increase divergence between the EU and UK

The approach of the Information Commissioner's Office (ICO) to enforcement, often favouring softer tools in the toolbox such as reprimands, will have a net effect of forcing businesses to take divergent approaches to data protection law compliance in the UK and the EU. We anticipate that this regulatory and commercial divergence will continue, creating both opportunity but also complexity for businesses. The UK's data protection regulatory regime has historically had a reputation as a more pragmatic, business-friendly regime, especially compared with some EU jurisdictions, where the enforcement of data protection law has been more dogmatic. The ICO has continued this more pragmatic approach as evident, for example, in its approach to consent or pay models and conducting transfer impact assessments following the Schrems II decision.

3. CrowdStrike incident will prompt system and supply chain cyber incident discussions

Representing one of the most significant global technology outages since NotPetya in 2017, the CrowdStrike incident will act as a poster child to prompt policyholders and insurers to review their policy wordings and coverage where a systemic or supply chain cyber incident has the potential to cause a massive financial impact. Coverage for non-malicious cyber events, including 'system failure' cover, is not always available or purchased by policyholders, and the CrowdStrike incident highlights its need. The CrowdStrike incident acts as a useful case study to review appropriate interruption periods, 'waiting periods' and retentions for non-physical damage BI cover, if purchased. It also prompts future discussion as to where the line is drawn between a policyholder's software and systems, and a managed services provider. Policyholder reliance on systemically important and vulnerable systems is continuing to increase beyond infrastructure and the cloud, challenging insurers to determine appropriate coverage limits and value appropriate premiums.

4. Cyber security laws will gather pace to keep up with technological developments and the evolving threat landscape

Digital threats are becoming increasingly common, more sophisticated and more impactful as society's digital transformation continues and there is an ever-increasing dependence on digital technology. As a result, cyber security laws will increase both in number and extent. At a UK level, we have already seen the Cyber Security and Resilience Bill introduced in the Labour government's first King's Speech. The Bill aims to "strengthen the UK's cyber defences [and] ensure that critical infrastructure and the digital services that companies rely on are secure" and will expand existing regulations to cover "more digital services and supply chains". In parallel, in September 2024, the UK government classified UK data centres as 'Critical National Infrastructure', a step designed to improve the security and resilience of these engines of the modern economy. Similarly, in the EU, the requirements of the revised Network and Information Systems Directive (NIS2) had to be implemented by EU members states by 17 October 2024, replacing the outdated laws implementing NIS1.

5. Privacy laws will slow the pace of AI developments

AI capabilities have developed exponentially in the past two years. In particular, advances in generative AI have resulted in this technology leaping to the top of board room opportunity and risk agenda and into the minds of the general public. However, it appears that the roll out of AI systems across organisations has slowed, in part due to complex privacy considerations. As data protection regulators continue to intervene, this trend will continue. As the privacy challenges arising from the use of AI systems crystalise and the regulatory focus increases, the Data Protection Impact Assessment will emerge as a crucial data protection tool.

6. Data breaches will remain a major concern for data controllers

Threat actors will continue to breach defences and cause loss, with the human factor remaining the weakest part of organisations' security systems. The continued search for the best balance between system security and usability will allow for continued penetration of systems. New challenges such as AI-related scams will create further risk. Although tools such as multi-factor authentication make third-party access harder, with cloud-based systems and resilient back-ups aiding recovery, none represent a panacea. In the future, we anticipate that data will simply be stolen, compared to current trends where data is often encrypted and ransomed against publication. For consumers affected by these incidents, while bank redress schemes may offer some form of remedy, they may encourage threat actors to see data theft as a victimless crime. For businesses, however, there will be no such redress.

7. Data claims will need to evolve

In the absence of a more generous approach by the courts when assessing quantum and costs, the pursuit of data breach claims on behalf of individuals will prove to be a question of financial risk for claimant representatives. Recent decisions have demonstrated the difficulty in succeeding in data breach actions where minimal distress or loss has been caused to a claimant. Alternatively, claimant representatives may look to pursue actions on behalf of numerous individuals in a class action. However, these actions are by no means a guaranteed route to success. The decision in Farley v Paymaster saw a significant percentage of data breach actions in a mass claim dismissed for not meeting the appropriate threshold of seriousness, and Adams v Ministry of Defence demonstrated the challenges of using an 'omnibus' Claim Form, where multiple claimants are added to a single claim. The Civil Procedure Rule Committee is considering this method of pursuing multiple claims, and this route may be closed off or narrowed significantly upon further guidance. Nonetheless, we still expect that claimant practitioners will explore other avenues to pursue data breach actions in response to judicial guidance and other pressures, as they have done in the past.

insurance.dacbeachcroft.com

dacbeachcroft.com

Connect with us: DAC Beachcroft LLP

Follow us: DACBeachcroft