Data, Privacy and Cyber Predictions 2024

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

DAC BEACHCROFT

Member of **Legalign Global**

Data, Privacy and Cyber Predictions 2024

1. Data ethics will play a greater role in guiding the use of personal and non-personal data

We expect many organisations to begin codifying an approach to data ethics in a formal governance framework to guide not just whether they can use personal and non-personal data, but also whether they should use it. Ethical considerations around the use of data are increasingly coming to the fore, particularly in light of rapidly evolving developments around the use of AI. These considerations are not new. In the past they may have manifested informally, taking into account general considerations such as good outcomes for your customer base or employees, public perception, use of the 'cool v creepy' test and your organisation's 'inner conscience'. However, the ever increasing reliance on data has brought - and will continue to bring - about a greater responsibility on organisations to handle data responsibly (in the broadest sense) and deal with the moral challenges arising out of its use.

2. The UK will rebalance its 'pro-innovation' approach to AI regulation

We expect to see more action and guidance from the UK government and regulators on the management of the risks of AI, whether building on existing regulatory frameworks or implementing new measures. Organisations seeking to engage AI within their business will need to keep abreast of these developments. In recent months, there has been increased pressure on the UK government to shift from its 'pro-innovation' stance on AI towards a more balanced approach. An interim report by the Science, Innovation and Technology Committee on the governance of AI urged the government to "accelerate, not pause, the establishment of a governance regime for AI". Further recent recommendations for greater AI regulation have come from bodies such as the Trades Union Congress and the Ada Lovelace Institute. The UK government has already made a move in this direction through the launch of the Artificial Intelligence Safety Institute and we have seen countries around the world endorsing 'frontier' AI safety under the Bletchley Declaration.

3. Regulators will increasingly collaborate and expand their traditional functions in respect of AI and digital technology

The Financial Conduct Authority and Competition and Markets Authority will continue to play larger roles in the regulation of AI and digital technologies, and increasingly collaborate with the Information Commissioner's Office. These regulators are already working together as part of the Digital Regulation Cooperation Forum (DRCF) and will shortly launch a multi-regulator sandbox (the DRCF AI and Digital Hub) to support organisations in meeting regulatory requirements for digital technologies. Cross-collaboration is evidently in the minds of policymakers, with the Science, Innovation and Technology Committee interim report on AI governance also concluding that resolving challenges posed by AI "may require a more well-developed coordinating function".

4. The role of the data protection practitioner will increase in scope

The issues at the forefront of data protection governance have expanded significantly over the past year. At the same time, the role of the data protection practitioner is evolving to keep pace with business needs. As we look to the future, Data Protection Officers (DPO) will increasingly find themselves being asked to opine on considerations outside the confines of the General Data Protection Regulation and Privacy and Electronic Communications Regulations. Some will look to bring issues such as data ethics and governance of non-personal data within their remit. Others may decide to create new roles such as an AI Ethics Officer. However, given the challenges in determining who is best suited to oversee the likes of AI regulatory compliance, many organisations are likely to default to the DPO, at least in the short term.

Data, Privacy and Cyber Predictions 2024

5. Connected product legislation will create new risks for insurers of manufacturers and distributors

We predict future discussions within the insurance industry as to whether risks and claims associated with connected products legislation sit within cyber, product liability, technology errors and omissions coverage or whether they will justify an entirely new insurance class. Regulations under the Product Security and Telecommunications Infrastructure Act will come into effect in April 2024, aimed at ensuring that consumer-connectable products are more secure against cyber-attacks. Manufacturers, importers and distributors of such products will need to comply with new security requirements (including bans on default or easily guessable passwords) and provide adequate reporting systems and transparency on a product's security updates. Penalties for non-compliance include compliance, recall and stop notices and large fines up to £10mn or 4% of worldwide revenue. The recoverability of such fines under a policy will be subject to any exclusionary language and/or the usual 'illegality defence' and public policy doctrine(s) surrounding such matters. These are entirely new legal risks for manufacturers and distributors which may prompt discussions as to which insurance line is best suited to meet them.

6. The ICO will increase enforcement action

Under the UK GDPR (General Data Protection Regulation), the Information Commissioner's Office (ICO) has a range of enforcement powers at its disposal. These include reprimands, enforcement notices and civil monetary penalties. In recent years, commentators have been critical of the limited number of fines that have been issued relative to the number of breaches reported. This is in part due to the limited resources, both personnel and financial, available to the ICO. Another factor might also be the prospect of the ICO having to self-fund subsequent legal appeals of its fines, which can only act as a disincentive against enforcement. However, since 2022, the ICO has been entitled to retain up to £7.5mn a year of the fines it issues to pay for litigation costs. Although implemented in 2022, we predict that we will only now start to see the results, given it will have taken the first year to build up the fund before providing greater confidence in the issuing of fines or in enforcement appeals.

7. UK/EU data-related class actions will continue to focus on privacy rather than security breaches

While massive security breaches grab headlines, they pose a problem when it comes to establishing class actions (in the UK, representative actions). The security requirements of both the UK and EU versions of the General Data Protection Regulation (GDPR) are not absolute but require levels of appropriateness. This means that any security-based action presents a significant level of litigation risk as to whether a GDPR breach can be proven. Compare this to a non-security-related GDPR breach, such as failing to have correct consent mechanisms in place for processing children's data or marketing data, where the breach is binary. The data was either lawfully collected or not. There is no interpretation of appropriateness. In such cases, class actions can skip straight to establishing commonality of damage in order to determine a viable claim.

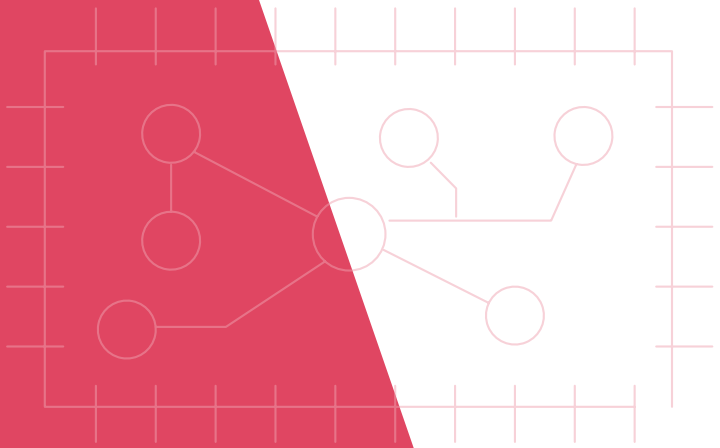
8. Low value breach claims will stack up

Claimant representatives will continue to try and circumvent small claims allocation for data breach claims in order to seek recoverable costs. This is despite the courts clearly indicating that low value data breach claims should be allocated to the small claims track and dealt with in the County Court. Recent trends have included data breach claims being pleaded as personal injury claims, with supporting medical reports submitted, in order to seek fast track allocation. These claims are not being submitted in the appropriate low value EL/PL portal, bypassing the fixed costs regime. Another trend is to 'stack' data breach claims together on one claim form, bringing the total damages sum above the small claims track threshold, circumventing existing group litigation mechanisms. There is some uncertainty as to whether these are appropriate routes for such claims to be brought and it is likely that future judgments will give greater clarity on these points.

Data, Privacy and Cyber Predictions 2024

9. Further exclusions for war and cyber operations will emerge

We predict further exclusions will be circulated and this topic will continue to generate controversy. At the time of writing, 29 'approved' clauses have been published by the LMA, and we know of more to follow. In addition, there may be as many variants that have not been published. This represents a huge change since the first LMA clauses were finalised in November 2021. Despite their proliferation, the clauses have yet to resolve all issues to the satisfaction of all participants in the cyber market. While we expect convergence over time, we anticipate that further iterations will yet emerge as the issues are debated. As and when the clauses result in judicial interpretation, in whatever jurisdiction, further scrutiny can then be expected.



insurance.dacbeachcroft.com

dacbeachcroft.com

Follow us: @DACBeachcroft

Connect with us: DAC Beachcroft LLP

Follow us: DACBeachcroft