BCLP. Client Intelligent

Insights

CYBER SECURITY TRENDS: TIPS FROM RECENT UK ENFORCEMENT ACTIVITY – PART 3

Mar 27, 2020

Key to recent ICO decisions has been the ICO's assessment of the extent and quality of communications with affected individuals and the regulator itself. It is clear the ICO sees certain behaviours (such as the setting up of call centres after a significant data breach) as minimum requirements in many cases involving well-resourced companies. It is an open question whether there is an onus on affected businesses to go further in demonstrating the rigor and effectiveness of their response to a data breach, and if so, what form this should take.

WHO IS THIS RELEVANT FOR?

For our Cyber Security Trends we reviewed recent findings to provide easy to use tips. Cyber incidents are sector and geography agnostic. These briefings draw on UK adjudications but are relevant for a GDPR-focus outside the UK and highlight cyber security trends more generally.

TIP: Informing individuals – don't expect much credit for achieving the industry standard

If the personal data breach is of a kind which triggers a requirement to inform affected individuals (likely to result in a high risk to their rights and freedoms), then notification on an individual basis (e.g. email), possibly supplemented by advertising will be expected. In addition, setting up a call centre and offering credit monitoring services, where financial data are at risk, as well as liaising with financial institutions like acquiring banks, are all par for the course. In one decision, the ICO noted critically that, while an organisation offered credit monitoring services, it had failed to communicate that effectively (as it should have done), which was evidenced by the fact that only a very small number of affected customers did so.

Drawing heavily on the extensive experience from the US of managing and responding to reported data security breaches at a state level, there is a fairly well-established range of assistance which organisations are expected to provide to individuals. Even though the GDPR does not provide any detail, e.g. there is no mention of whether, when or how telephone hotlines should be provided, the ICO appears to expect such measures to be offered in large scale breaches.

What sanctions apply?

In the UK the ICO can fine up to 4% of annual global turnover or £17,500,000 whichever is higher. There are related powers to compel actions to be taken, information to be provided and to conduct on site assessments and interviews.

Brexit Postscript

Once the UK has finally left the EU at the end of 2020, organisations impacted by cyber security breaches face an increased risk of multiple fines and enforcement actions for the same incident. This is because the UK ICO will no longer participate in the GDPR cooperative “one stop shop” mechanism alongside its European counterparts.

As the UK’s ICO is the one of the largest and best-resourced data protection authorities in Europe, with a proven track record of enforcement, companies with pan-European operations cannot afford to take their eye off the UK.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Geraldine Scali

London

geraldine.scali@bclplaw.com
+44 (0) 20 3400 4483

professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.