BCLP. Client Intelligent

Insights

CYBER SECURITY TRENDS : TIPS FROM RECENT UK ENFORCEMENT ACTIVITY – PART 5

Jun 29, 2020

In this part of our briefing series, we look at how individual reactions to a data breach can shift the dial from a regulator's perspective. Recent decisions have shown that the ICO will look behind a company's public statements to scrutinise the substantive impact of any remedial measures offered to individuals. The impact of your public communications and the reality of your mitigating efforts have arguably never been more important.

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: Individuals' complaints and reactions to the breach can affect the fine

The ICO will take account of complaints it receives from individuals about a personal data breach, typically after they have been notified by the company about it. The regulator will also want to know how many complaints the company received directly. These complaints are relevant to assessing the seriousness of the breach, in terms of the distress or other damage it causes individuals. It could also affect the ICO's view of the organisation's mitigation efforts, for example, if your customers are complaining that they don't know what they should be doing or how to protect themselves, then part of your mitigation efforts may be judged to be inadequate (like offering credit monitoring but not making it clear who to contact in order to get this).

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
