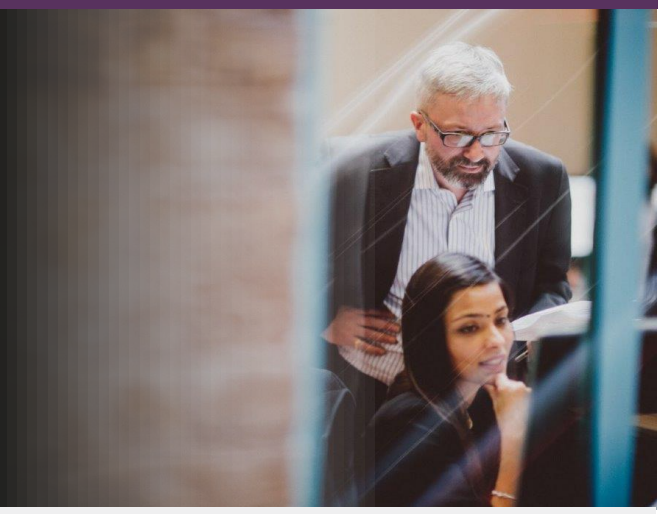
RIAA Barker Gillette

Always Available

Fines fly following airline cyber breach



July 2019

The news that British Airways is facing a fine of £184m after personal data of some 500,000 customers was harvested by cyber criminals shows the tough stance of the UK's data regulator following the introduction of new EU data protection laws last year.

The General Data Protection Regulation (GDPR) has seen stricter operating boundaries for businesses processing personally identifiable information about individuals, and it also ushered in extended powers for data regulators, which is the Information Commissioner's Office (ICO) in the UK. Under the previous regime, the maximum penalty for data breach was £500,000, but following the introduction of GDPR in May 2018, fines of up to €20m, or 4% of total worldwide turnover, can be imposed on businesses.

Robert Baugh, the CEO of Keepabl, recently wrote in the Modern Law Magazine an article highlighting the wider costs companies can face in remedying any breach. Baugh writes: "…the fines for the breach are likely to be dwarfed by other costs" and in the example given these costs outweighed a German company's fine by 4 to 1.

For British Airways, unwitting customers were diverted from the real BA website to a fraudulent site, but even though the breach was not on their website, the investigation by the ICO found poor security arrangements by BA had compromised customer data, including log in and payment details, as well as names and addresses.

Our Data Protection Leader, Qaiser Khanzada, explains:

"It's up to BA to make representations to the regulator over the findings to see if they can demonstrate why the proposed fine should be reduced, but this is a clear sign that the ICO is not going to pull any punches over data breaches under the new regime."

The aim of GDPR was to harmonise data protection across all EU member states, meaning that any UK business trading with EU citizens must comply, both now and after Brexit. It introduced a statutory obligation to notify the regulator of any breach which placed an individual's personally identifiable information at risk and the ICO has recorded more than 40,000 data protection complaints since the launch of GDPR, with 14,000 personal data breaches reported.

The head of the ICO, Elizabeth Denham, has urged organisations to face up to the challenge and move beyond baseline compliance to accountability, with evidenced understanding of the risks to individuals in the way they process data, and focused attention on how to mitigate those risks.

Qaiser added:

"It's a fast-changing environment. Just because you were confident about compliance when GDPR was introduced in 2018, doesn't mean you can ignore the new guidance that's coming through. Also, you need to take account of enforcement actions, to see where problems may arise.

And, although we still don't know what's happening over Brexit, what we do know is that whatever happens on that front, GDPR compliance will continue to be the minimum standard required of UK companies who wish to do business across Europe."

Reviewing your GDPR compliance

Check your policies and procedures

Stress test your processes on a regular basis, and review whether policies are clear and easily followed. If not, they should be revised and clarified. If the way you operate has changed, this could impact GDPR compliance, and policies need to be regularly updated to reflect recent changes, such as the guidance on transparency and consent from the European Data Protection Board.

GDPR refresher training

Regular enactments of mock data breaches can help keep GDPR at the forefront for staff, as well as identifying where changes may be needed. Whenever policies need to be updated, make sure refresher training is conducted with relevant staff, and with detailed development training for any staff who are frontline on data management. Regular training is one of the things that the regulator will be looking for, if anything does go wrong.

Reporting

Staff should be encouraged to seek out, recognise and report data incidents, so make sure you have the right culture that encourages open reporting. The regulator wants to see prompt identification and reporting, as the longer it takes to identify a possible data breach, the more likely that a situation will mushroom out of control.

Third party relationships

If you transfer personal data through third parties, such as suppliers, or transfer it outside the EU for any reason, it's important that all related contracts and processes comply with GDPR requirements.

Data Protection Impact Assessments

Make sure you understand the circumstances in which you are required to conduct Data Protection Impact Assessments. These are key to the GDPR philosophy of designing systems with privacy at their heart and should be undertaken whenever data processing could result in a high risk to individual rights and freedoms. Guidance on the ICO website sets this out in detail.

if you have any queries, contact Qaiser Khanzada today.

Qaiser Khanzada
020 7299 6901
qaiser.khanzada@riaabg.com
www.riaabarkergillette.com

Click here to make an appointment