Browne Jacobson

If you think data compliance is expensive – try having a data breach!

28 June 2023

Previous
The FM Global Resilience Index 2023: underwriter risks

News has recently been published that is beginning to reveal the potential scale and impact from unauthorised third party access to insurance systems and databases hosted by consulting and digital services business, Capita, in March 2023. Over 90 organisations who use Capita's services have reported their breaches to the ICO. Capita already expects to incur operational costs up to £20m associated with the cyber incident, before any regulatory sanction is imposed in addition, and any resultant loss of business is realised.

Are you at risk?

Capita are a market leader in outsourced tech services. Aviva and Phoenix (both insurance clients of Capita) have already both been named as affected insurance entities.

It may seem harsh that if you legitimately onboard with an outsourced tech services provider who becomes subject to a targeted, malicious cyber attack by professional criminals, then you could somehow remain liable to the data subject for the loss of their data even where it was your provider who was hacked. The EU GDPR in 2018 changed this. De-risking that outsourcing process, including the contract that underpins it, therefore becomes ever more important. You may need to consider your existing contractual position for your existing provider, if you haven't already.

Where you have outsourced your data hosting services to a third party, whilst you won't get fined by the ICO for a data breach by that third party that wasn't your fault, the FCA may want to know about the systems and controls you have in place to protect customer data, and you are at risk of compensation claims from data subjects whose data has been compromised Whether you have a right of recovery against the third part supply will depend on the contractual terms in place.

Naturally, if you do not currently use Capita, you won't be affected by this particular incident, but it certainly highlights that no-one is immune from such threats, and any organisation could be targeted next.

If you aren't sure where the personal data you process is, or how robust your cyber infrastructure is, now might be a sensible time to start undertaking a data audit. ICO guidance is widely available online (for free). Legal support is also readily available.

What should you do now?

The Capita incident clearly highlights the real risk of doing modern business, and the insurance industry in particular thrives on data hosted on a cyber infrastructure.

Of course, if you are a client of Capita's, you will probably already be aware of the recent incident(s) and what personal data (if any) has been affected.

Regulatory investigations into the incident are ongoing and will continue for some time. From there, it will become clear what the potential regulatory sanctions may be, which will undoubtedly be of interest to any organisation that outsources their data to a third party processor (insurance, or otherwise).

The FCA has instructed potentially affected regulated entities to undertake systems checks for potential fallout and to assess whether to notify impacted customers, suppliers or colleagues. Impacted services were only restored some 10 days after the initial event, and initial reports are indicating that, thanks to containment, limited volumes of data on Capita's servers was exfiltrated and leaked (anywhere between 0.1% and 4% have been published). No doubt the extent of the breach has not yet been fully realised.

The potential scale of this widely publicised fallout could be significant. The ICO's published statement is available here, along with Capita's here. The ICO is also inviting breach reports to be submitted. Further fallout, and regulatory sanctions, are sure to follow. If you have any questions relating to this ongoing incident, which is no doubt of substantial concern, the ICO are able to help. Alternatively, contact your legal adviser(s).

Contents

Key contact

Tim Johnson

Partner

tim.johnson@brownejacobson.com

+44 (0)115 976 6557

Related expertise

Services

Coverage disputes and policy interpretation

Policy drafting and distribution