wiggin

British Airways Fine

In this video, I'm going to discuss the British Airways data breach and the resulting fine which was issued. You may have heard the BA fine referenced for a few reasons:

Firstly, it's currently the largest fine ever issued by the ICO at 20 million pounds.

Secondly, it was substantially reduced from the original 183 million pounds intended to be fined.

And thirdly, the data breach affected more than 400,000 BA customers and so there's a good chance that you or someone you know may have been affected.

So what happened?

In 2018, British Airways suffered a significant data breach. The breach resulted in traffic to the BA website being diverted to a fraudulent site, where personal information of approximately 400,000 staff and customers was harvested. This continued between June and September 2018 without causing any disruption to BA's usual booking procedures.

As a result, BA breached the GDPR by failing to comply with the security and accountability principles.

In its investigation, the ICO found the security measures BA had in place to prevent cyber-attacks were inadequate when considering the huge volumes of personal data being processed. BA failed to protect itself and subsequently did not detect the attack for more than two months.

Infringements of GDPR can lead to fines of up 20 million euros or 4% of total global turnover, whichever is higher. After a thorough investigation in 2019, the ICO issued a notice of its intention to fine BA an eyewatering 183 million pounds.

BA and the ICO then engaged in negotiations around the severity of the penalty.

The ICO considered BA's mitigating factors as well as the economic impact of COVID-19 on the organisation. This resulted in the ICO announcing on 16 October 2020 that the BA fine had been reduced to 20 million pounds.

There are a few key messages to take away from the BA investigation.

Firstly, appropriate and proportionate security is vital, with encryption suggested for all data held, not just payment data. The ICO's report emphasised that regular reviews and testing of security systems are essential to ensure they are adequate and fit for purpose.

Secondly, the reduced fine proves that cooperation with the ICO and any other relevant government or regulatory bodies is critical when handling a breach alongside taking prompt effective remedial action.

Finally, the BA case has demonstrated that providing robust representations in response to initial fines can be commercially advantageous.