The Information Commissioners Office flexes its muscles: first fines under the GDPR

After much speculation about what the first fines issued by the Information Commissioners Office might be we have seen two significant statements of intention to fine in the same month

06 August 2019

After much speculation about what the first fines issued by the Information Commissioner's Office ('ICO') might be, we have seen two significant 'statements of intention' to fine in the same month. Both were issued against large corporate companies but have much wider relevance, especially in the context of the health sector given the volume of sensitive information being processed by health organisations.

In addition to these two proposed GDPR fines, earlier in the year the ICO issued a sizeable fine under the Data Protection Act 1998 ('DPA 1998') in the context of filming on a hospital site, providing a further reminder of the requirements for valid consent and the importance of adequate transparency information. The reputational damage suffered by each organisation as a result of these incidents should also not be discounted when assessing impact.

Fine - True Visions Productions

In April 2019 the ICO fined True Visions Productions ('TVP') £120,000 for unfairly and unlawfully filming patients at a maternity clinic. This fine was awarded under the DPA 1998 as the breaches occurred prior to the General Data Protection Regulation ('GDPR') coming into force.

TVP, a television production company, had set up CCTV style cameras and microphones in examination rooms at a walk in clinic for patients with concerns about their pregnancy for a Channel 4 documentary relating to stillbirths. TVP had the consent of the clinic.

The ICO found that TVP had failed to comply with the requirements of the DPA 1998 to process personal data fairly and transparently as they had not provided patients with adequate information about filming which took place over a 4 month period. They also failed to get adequate permission from those affected by the filming in advance.

Whilst TVP had posted some notices near to cameras and in the clinic waiting room, as well as leaving letters on waiting room tables, the ICO found that these did not give sufficient information to patients about the filming. TVP did not directly and specifically inform patients that they would be filmed. The notices and letters were generalised and did not properly inform patients about the processing of their personal data.

No consent was obtained from patients in relation to the filming. There was no mechanism by which cameras could be stopped if patients objected to filming.

As the fine was issued under the DPA 1998, the maximum fine at the time was £500,000 and so the fine issued against TVP should be considered a fairly significant penalty. However, the strengthened requirements under the GDPR in relation to transparency and consent should be noted when considering this decision, which could well have meant a larger fine if the breaches had occurred post May 2018. It also highlights the need to ensure a data privacy impact assessment is carried out that incorporates practical considerations around how data protection obligations will be met.

Intention to fine - British Airways

On 8 July 2019 the ICO issued its statement of intention to issue a fine of £183m to British Airways in respect of breaches of its security systems. The incident involved user traffic being diverted away from the BA website to a fraudulent site where customer details were harvested. The breach involved the personal data of around 500,000 customers between June and September 2018. The personal data involved included log in, card payment and travel booking details as well as name and address information.

The ICO's investigation revealed poor security arrangements on the part of BA, with the Information Commissioner sending a warning to all organisations handling personal data that *"the law is clear – when you are entrusted with personal data you must look after it. Those that don't will face scrutiny from my office to check they have taken appropriate steps to protect fundamental privacy rights"*.

The security failings by BA included the lack of appropriate system updates and monitoring, which exposed the vulnerabilities that resulted in the breach. These were noted in the Lessons Learned Report into the WannaCry Ransomware Cyber Attack (Lessons Learned Review of the WannaCry Ransomware Cyber Attack, 1 February 2018) as vulnerabilities within the NHS in England.

The WannaCry attacks *"exposed a need to improve across all parts of the NHS, including improved discipline and accountability around cyber security at senior leadership and Board level, the importance of swift and effective patching of systems when new security updates are released, and historic underinvestment in network security and up to date software"* (paragraph 1.8). The proposed BA fine is a reminder of the seriousness of cyber and data security and accountability.

Intention to fine - Marriott

The following day the ICO issued a further statement of intention, this time to issue a fine of £99m to Marriott International Inc for breaches of the GDPR. The fine relates to a cyber incident notified by Marriott in November 2018 in which various personal data contained in approximately 339 million guest records globally were exposed. This included around 30 million EEA residents.

Significantly, the vulnerability of the relevant systems began in 2014. At this time the systems belonged to Starwood hotels group, which was subsequently acquired by Marriott in 2016. The breach was not identified until 2018.

The ICO found that Marriott had failed to undertake sufficient due diligence when it took on Starwood. It was also found that Marriott should have done more to secure its systems.

Under the GDPR, organisations must be accountable for the personal data they process. This includes ensuring that whenever a third party is involved, whether by way of an acquisition of that third party or otherwise, appropriate due diligence must be undertaken. To fail to do so risks substantial financial penalties from the ICO. This again is a timely reminder for health organisations in a period of significant organisational change to ensure that careful due diligence is carried out and that any issues identified are appropriately addressed, with a clear audit record being kept of the measures taken.

If you would like to discuss any of the issues discussed above or data protection more widely, please contact Charlotte Harpin.

Contact

Charlotte Harpin

Partner

charlotte.harpin@brownejacobson.com

+44 (0)330 045 2405

Related expertise

Services

Data protection and privacy

Intellectual property

Reputation management