December 20, 2018

The Sky's the Limit: The Cathay Pacific and British Airways Data Hacks, and the GDPR Six Months On

Cathay Pacific, the Hong Kong airline, is the latest airline to face a cyber-attack; in this case, one that has resulted in the theft of personal data of up to 9.4 million passengers. The hackers gained "unauthorised access" to Cathay Pacific's passenger data systems and accessed personal data, including passport numbers, Hong Kong identity card numbers and credit card numbers. There is currently no evidence of the misuse of this information; however, as with all data breaches, this evidence—and the awareness of them by the affected individuals—often takes time to emerge.

With multiple recent incidents involving another carrier, British Airways, the airline industry finds itself in the spotlight, facing questions as to how it will react to these breaches, and how it will address data security concerns moving forward. British Airways was first hit earlier this year with an IT incident in their data centre that grounded all their flights from London's Heathrow airport for a day. The UK airline then faced another crisis in September 2018, issuing a warning that a computer hack had compromised credit card and personal data from customers who had made reservations on its website and mobile app. Further, whilst investigating this breach in October, British Airways discovered yet another breach that had occurred between April and July, potentially affecting more than 185,000 people.

Cathay Pacific and British Airways will both face scrutiny by the authorities as well. Although the UK Information Commissioner's Office (ICO) has not yet taken any enforcement action in relation to these incidents, each involves a serious data breach affecting personal data within the scope of the EU General Data Protection Regulation (GDPR) that could result in large fines. Further, given the large number of people who have been affected, it will be interesting to see whether Article 82 of the GDPR will come into play, which gives grounds for any person to receive compensation if they have suffered material or non-material damage as a result of a personal data breach.

Data incidents are not just limited to airlines, however. In November, the ICO fined Uber £385,000 for failing to protect its customer's personal data information during a series of cyber-attacks in October and November 2016[1]. This incident highlights that how one deals with a data incident is as important as the data incident itself. The ICO condemned the fact that Uber failed to inform the customers and drivers affected for more than a year, stating: "this was not only a serious failure of data security on Uber's part, but a complete disregard for the customers and drivers whose personal information was stolen. At the time, no steps were taken to inform anyone affected by the breach, or to offer help and support. That left them vulnerable"[2].

[1] ICO news, "ICO fines Uber £385,000 over data protection failings".

[2] ICO news, "ICO fines Uber £385,000 over data protection failings".

For more information, please contact the following or any members of Katten's **Privacy, Data and Cybersecurity** practice:

Alan D. Meneghetti
+44 (0) 20 7770 5232
alan.meneghetti@kattenlaw.co.uk

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

Joshua A. Druckerman
+1.212.940.6307
joshua.druckerman@kattenlaw.com

Yasmin Roland
+44 (0) 20 7776 5245
yasmin.roland@kattenlaw.co.uk

In October, Eurostar (the UK-Europe train company) also suffered a near miss with a data incident, reporting to customers that an "unauthorised attempt" had been made to hack into its systems and access customer's personal accounts. Eurostar confirmed that credit card details and payment details were not, however, compromised, but has advised customers to reset their passwords. An ICO spokesman confirmed that they were making enquiries into Eurostar's report.

Enforcement by the ICO Under the GDPR

Whilst we do not yet know what level of fines will result from the first enforcement actions under the GDPR, the ICO appears to be gearing up for a more robust approach than has been seen in recent years. The ICO has projected that it will be expanding its workforce by at least 30 percent over the course of the next few years[3] to assist its current employees who are already shouldering the increased workload following the GDPR coming into force in May 2018.

The first UK enforcement notice under the GDPR and the new UK Data Protection Act 2018 (DPA 2018) was served on 6 July 2018.[4] In addition to being the first action taken under the DPA 2018 by the ICO, it was served on AggregateIQ Data Services Ltd (AIQ) and marks the first time that the ICO has attempted to take enforcement action outside the jurisdiction of the UK. AIQ, a Canadian data firm, uses data to target online ads at voters during public polls, and was notable for its activities promoting the "Leave" movement. As AIQ's processing of personal data relates to the monitoring of data subjects within the EU, it is subject to the GDPR.

In its enforcement notice, the ICO alleges that AIQ processed personal data in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing. Furthermore, AIQ's processing was arguably incompatible with the purposes for which the data was originally collected.

Many are eagerly awaiting a decision, with this enforcement being the first of its kind that can result in the GDPR fines of up to EUR 20 million or 4 percent of annual global turnover (whichever is higher).[5] However, AIQ has exercised its right of appeal to the First-tier Tribunal under section 162(1)(c) of the DPA 2018, and so commentators and interested parties will have to wait a little while longer for a final decision.

For the First Time, ICO Issues Two Maximum Fines Under the UK Data Protection Act 1998 (DPA 1998)

Companies have already seen a change in attitude from the ICO since the GDPR went live in May; despite being issued under the old regime, enforcement fines have almost doubled in the year ending September 2018. In addition, ICO has issued two £500,000 fines in 2018 (the maximum available to the ICO under the DPA 1998), which is notable because the maximum fine had never been imposed previously.[6] It is expected that a more robust approach will be taken by the ICO, with fines being issued on a much quicker turnaround than under the DPA 1998 where it was not uncommon for a fine to be issued years after a breach took place.

The ICO imposed one of these £500,000 maximum fines against Equifax Ltd on 20 September 2018, for its failure to protect the personal information of up to 15 million UK citizens during a cyber-attack in 2017.[7] As noted above, the fine was issued under section 55A of the DPA 1998 as the breach occurred before the entry into force of the GDPR and the DPA 2018.

The ICO imposed the second maximum fine against Facebook in October 2018[8] for an incident that took place prior to the implementation of the GDPR for a failure to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data (under Principle 7 of the DPA 1998) in permitting apps and developers, including Cambridge Analytica, access to personal data.

---

3 ICO Resource and Infrastructure Strategic Plan.

4 ICO, AIQ Enforcement Notice.

5 Article 83 GDPR.

6 ICO, Information Commissioner's Annual Report and Financial Statements 2017–18.

7 ICO, Data Protection Act of 1998 Supervisory Powers of the Information Commissioner Monetary Penalty Notice.

8 ICO news, "ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information".

These fines, although issued under the DPA 1998, highlight the type of, and basis for, enforcement actions that the ICO is willing to take. Further, by issuing two maximum fines in 2018 (when the maximum fine had never been issued previously), they also serve as a cautionary reminder to companies that the ICO is willing to use the powers available to it to the maximum extent, which is particularly worrisome given the increased maximums available under the GDPR. Considering the scale of the British Airways breaches, it will be interesting to see whether the ICO continues this approach and issues a fine in the region of the maximum available to it under the new legislation.

ICO Publications on Reporting Personal Data Breaches Under the GDPR

Article 33(1) of the GDPR imposes a new general requirement on data controllers to report personal data breaches they have suffered to the relevant supervisory authority "*without undue delay and, where feasible, not later than 72 hours after having become aware of it*." The ICO released statistics showing they received 1,792 notifications of data breaches in June 2018—over four times the number of breaches notified in April 2018.[9] The ICO has, however, described a situation where data controllers are 'over-reporting' due to the fear of not complying with their obligations under the GDPR, and has advised that data controllers should focus on maintaining their own internal record of data breaches that do not meet the notification threshold, including their reasoning as to why the threshold was not reached.[10] However, it should be noted that the GDPR (and its 72-hour timeline) does encourage this kind of over-reporting; many data controllers may find it easier, and less risky, to report with incomplete information rather than become subject to an enforcement action for failing to report within the specified time period.

In response to this over-reporting, the ICO has also released information highlighting that there has been an increase in a number of reports that are not compliant with the legislation; for example, where data controllers have a lack of understanding into whether a personal data breach has actually occurred.[11] Per the ICO, companies should be aware that notifications should only be made when the threshold for "personal data breach" has been reached. The ICO also commented that personnel with suitable seniority and clearance need to be able to give as much detail in relation to the breach and when the ICO can expect the remaining information.

---

9 ICO, Data Breach Reporting Webinar.

10 ICO news, "ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference".

11 ICO news, "ICO Deputy Commissioner (Operations) James Dipple-Johnstone – speech to the CBI Cyber Security: Business Insight Conference".

Katten

Katten Muchin Rosenman UK LLP

www.kattenlaw.co.uk

Paternoster House, 65 St Paul's Churchyard • London EC4M 8AB
+44 (0) 20 7776 7620 tel • +44 (0) 20 7776 7621 fax