Client Alert | Data, Privacy & Cybersecurity / Technology

UK ICO continues heavy GDPR enforcement trend with £99m fine

July 2019

Authors: John Timmons, Tim Hickman

The UK Information Commissioner's Office has announced its intention to issue a £99 million fine to a global hospitality business, in respect of a personal data breach under the GDPR. This comes a day after the ICO announced its intention to fine British Airways £183 million for a personal data breach of a similar nature. The message is clear: non-compliance with the GDPR carries the risk of significant financial penalties for businesses in all sectors.

Enforcement of the General Data Protection Regulation ("**GDPR**") began more than a year ago, and Data Protection Authorities ("**DPAs**") across the EU are now beginning to issue significant fines for non-compliance. Failure to comply with the GDPR can result in regulatory investigations, fines, and damages claims, all of which could undermine trust and confidence among consumers and investors. DPAs have the power to issue fines of up to €20million or 4% of annual global turnover (whichever is greater) for each breach of the GDPR. It is now clear that European DPAs are willing to make use of this power to impose significant financial penalties.

The UK DPA, the Information Commissioner's Office ("**ICO**"), has issued two notices this week outlining its intention to fine a global hospitality business £99 million, and a similar intention to fine British Airways £183 million, for allegedly failing to adequately safeguard personal data. The ICO's action comes a few months after the French DPA issued a similarly significant €50 million fine against a US-based tech business for allegedly failing to provide sufficient information to its users regarding the collection and use of their personal data and failing to obtain valid user consent.

Several of the most high-profile data protection enforcement actions in recent times have been carried out against tech businesses. This had led some businesses in other sectors to wrongly believe that GDPR compliance was primarily a problem for the tech sector, and that businesses in other sectors were exposed to lower risks. By issuing two record fines in successive days against non-tech businesses, the ICO has sent a very clear warning that any business that breaches the GDPR, regardless of the sector in which it operates, is at risk of enforcement.

These enforcement actions also offer an insight into the level of fines that businesses can expect to face should they fail to satisfy the requirements of the GDPR. Although the GDPR puts a very high ceiling on maximum fines, it offers very little context on what real-world fines could look like. In addition, because it took EU DPAs more than a year to issue serious financial penalties under the GDPR, there had been a hope in some quarters that such penalties would never materialise. The ICO's recent actions, which were taken in collaboration with other EU DPAs, clearly demonstrate that this hope was misplaced, and that real-world fines in the tens of millions are to be expected.

Business should consider this a timely reminder to revaluate their GDPR risk exposure. Businesses should review policies and procedures implemented in the run-up to the implementation of the GDPR and ensure these continue to be effective in supporting compliance and protecting personal data. Data security measures

implemented to safeguard personal data should be subject to continual review to ensure that they remain effective against current known threats and vulnerabilities.

Businesses operating in the UK (or targeting the UK market) should be familiar with the key points from the ICO's Regulatory Action Policy ("**RAP**"). The RAP sets out the ICO's five-year programme of key regulatory priorities and is intended to enable businesses to predict how the ICO will carry out its regulatory activity. The RAP includes guidance on the approach the ICO will adopt when considering whether to issue penalties to businesses. Some of the key factors considered by the ICO are as follows:

- the nature, gravity and duration of the failure;
- the sensitivity of the data involved;
- whether there has been a degree of damage or harm (which may include distress and/or embarrassment);
- the degree of responsibility of the business;
- whether there has been a failure by the business to implement the accountability provisions of the GDPR;
- any relevant previous failures; and
- the manner in which the ICO became aware of the incident

This is the first wave of significant enforcement action since the introduction of the GDPR and it suggests that DPAs are willing to impose substantial fines on businesses that they determine to be in breach of data protection law, regardless of the sectors in which those businesses operate. We anticipate further fines, of a similar or higher value, to be issued in the second half of this year and we expect to see a surge in the number of individuals brining private actions against businesses regarding GDPR non-compliance.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000