By Ben Symons

Protecting the personal data of both customers and employees by organisations is a hot topic. The Cambridge Analytica scandal has pronmpted action both the European Commission and UK governments to enact legislation to make data protection a top priority.

A data breach has a number of significant legal consequences

Obligation to report the data breach

The UK recently enacted the Data Protection Act 2018 (DPA). The DPA requires an organisation to:

(1) Report any data breach to the Information Commissioners Office (ICO) within 72 hours;

(2) Notify the individual who is the subject of the data breach.

Fines and penalties from the ICO

A data breach will trigger an investigation by the ICO Under the DPA, the ICO can levy fines of the higher of:

(1) £20 million; or

(2) 4% of the worldwide turnover of a corporate group.

In 2015, the ICO issued Carphone Warehouse a fine of £400,000 for a data breach involving 2.5 million customers. This may seem trivial, however, the maximum fine that the ICO could issue at the time was £500,000.

The ICO can clearly issue much larger fines under the DPA. This should be a real concern to Marriott or any other organisation suffering a serious data breach.

Legal action by individuals

Under the DPA and at common law, individuals who are the subject of a data breach can take legal action for:

(1) Financial loss;

(2) Distress, anxiety and their loss of privacy.

In cases where credit card information of individuals is leaked by an organisation, there is clearly the potential for financial loss by the individuals concerned and significant damages claimed.

In 2018, a class action was started against British Airways seeking around £1,200 for 380,000 customers who had been the subject of a data breach. British Airways could potentially be liable for around £500 million in damages (although this figure is likely to be smaller if the matter is settled).

In 2016, Mitting J in *TLT and others v Secretary of State for the Home Department and Home Office [2016] EWHC (QB)* ordered the home office to pay asylum seekers around £7,000 each as a result of mistakenly publishing private information of these individuals on its website.

Conclusion

The security and proper use of data relating to individuals should be a top priority for all organisations, whatever their size. Data breaches are a hot topic. A data breach is embarrassing and reputationally damaging.

Increasingly, data breaches are resulting in serious financial penalties and all organisations need to make preventing data breaches a top priority.

Ben Symons
36 Commercial
https://36group.co.uk/members/bs

36 Commercial
Key Contacts:

Steven Newbery (Commercial Practice Manager)
steven@36commercial.co.uk
Tel: +44 (0) 207 421 8051
Mobile: 07786 023 245

George Scanlan (Commercial First Junior)
George@36commercial.co.uk
Tel: +44 (0)202 421 8051

https://36group.co.uk/commercial