4 September 2017

insider.co.uk

From 25 May 2018 the **General Data Protection Regulation** will be enforced. This enhances the rights of data subjects putting them back in control of their personal data and provides more obligations for data controllers to assist with this.

To enforce this, the Regulator, in the UK the ICO, gets more powers to ensure that companies are

The maximum fine will be €20 million or 4 per cent global turnover and fines can be imposed for breaching the data protection principles but also for failing to have the correct administrative procedures in place - i.e. failing to report a breach which can attract an additional fine of up to €10 million or 2 per cent global turnover.

In addition there is an obligation to report some data breaches involving personal data being lost, altered, destroyed, accessed either accidentally or unlawfully. If there is likely to a risk to the rights and freedoms of an individual then they must be reported to the ICO within72 hours of being discovered.

In addition if there is likely to be a high risk to the rights and freedoms of individuals then the breach must be reported to the data subject whose information has been affected.

What GPDR would mean for 'hacked' Equifax and Deloitte

In September 2017, **Equifax**, the US Credit Reporting firm, confirmed that it had been hacked leaving the data of 143 million American citizens vulnerable along with the data of 400,000 individuals from the UK and Canada.

Later in September Deloitte also admitted that their systems had been hacked compromising personal data – Deloitte insisted that it was only personal email addresses and that only a very few customers were affected.

Clients affected were advise, but it appears that this attack was discovered in March but was only confirmed in September. It may have occurred earlier than March.

What impact would the GDPR have on these organisations if these breaches happened post-May 2018?

The GDPR has a wide geographical reach and any organisation who is processing the data of someone in the EU has to comply.

Therefore post-May 2018, Equifax would be obliged to report this breach and would face fines of up to 4% global turnover if, as it appears, it did not have the appropriate measures in place to ensure that its system was patched allowing a vulnerability to be exploited.

Given the resources available to an organisation the size of Equifax, I doubt the ICO would hold back in issuing a significant fine here. Up to 4% of its $3.1 billion turnover amounts to $124 billion or €106 million.

In relation to the Deloitte breach, it appears that they took almost a year to identify a breach and what is significant about this breach is that Deloitte is one of the 'Big Four' accounting firms in the World and it provides cyber security advice to their clients!

The system that was hacked was secured by a single password and no two factor authentication.

So a lack of appropriate security measures could lead to a maximum fine of $156 billion but in addition there could also be a fine in relation to failing to report the breach of up $78 million.

And in addition, both companies are likely to face civil claims for compensation – no longer just in the US, but in the UK and EU too. The fines could be the tip of the iceberg ...

Laura Irvine is Partner and Solicitor Advocate for BTO Solicitors LLP