Data Protection Day—enforcement of Corporate Crime

27/01/2016

Corporate Crime analysis: Data Protection Day aims to raise awareness as to how data is used and explores the latest developments in data protection regulation. As part of our Data Protection Day series, Ian Whitehurst, barrister at 6 Pump Court, explains the area of corporate crime enforcement in light of the forthcoming General Data Protection Regulations (GDPR).

What fines and sanctions can businesses face for non-compliance?

The Information Commissioner's Office (ICO) is able to issue an enforcement notice compelling a business to remedy a breach of the Data Protection Act 1998. The sanction is made public, advertised on the ICO's website, and carries significant harm to the reputation of the company concerned.

Individuals and companies accused of stealing personal data face the sanction of criminal investigation and prosecution by the ICO, which leads, after conviction, to the imposition of financial penalties and the implementation of confiscation proceedings to deprive the offenders of their benefit from the criminality.

Have there been any noteworthy fines issued by the ICO to date? What has been the reaction to this?

The maximum financial penalty that can be imposed by the ICO is £500,000. In recent years, there have been significant fines, for example:

- a telecommunication company was fined £440,000 for sending spam text messages
- a green energy company was fined £200,000 for recklessly breaking marketing call regulations, and
- an NHS Trust was fined £325,000 when sensitive patient data was discovered being sold via eBay

In relation to personal data theft, a criminal court is limited to the imposition of financial penalties on offenders.

There is a growing awareness of the consequences of breaching and stealing personal data on a corporate and individual level. At present, the risk of detection and the financial penalties imposed on offenders has not apparently prevented the misuse of personal data.

In light of the reforms contained in the GDPR, it is anticipated that business awareness and understanding will have to increase dramatically to ensure regulatory compliance.

Are there any best practice tips available to help businesses avoid common mistakes which lead to enforcement action being taken?

Businesses need to consider and document what personal data is held by them, where it is held and what is actually being done with the personal data in their possession. If the material is highly sensitive in nature, consult with the ICO to develop and deploy compliant systems to manage the possession and retention of such material.

In addition, businesses need to consider:

- installing firewalls
- checking for viruses
- ensuring operating systems are automatically updated and security updates implemented
- preventing staff members from sharing passwords
- limiting access to various parts of the IT system to staff members
- encrypting personal data which is held by the business, and
- ensuring personal data is removed from computers before they are disposed of

It is important to remember the ICO has discretion on how to proceed in relation to each case and they may make recommendations to a business or seek undertakings from the business to ensure future compliance. The ICO can, of course, take matters further by issuing enforcement notices and in appropriate circumstances impose fines.

However, it is not an automatic process that a breach will lead to a fine being imposed, as can be seen from the alternative options available to the regulator. It must also be remembered that some breaches would be viewed as unforeseeable.

Do you predict that the GDPR and an anticipated increase in the level of fines issued will change the behaviour of businesses in relation to data protection?

The GDPR is going to force businesses to adapt to the new regulatory regime that it implements. Privacy and the protection of privacy by businesses must now be at the forefront of their consideration when dealing with data issues. Businesses will need to liaise and engage with the ICO over any concerns, queries or high-risk operations they are involved in.

If they do not adopt a proactive approach to the new regulatory regime, the new measures requiring compulsory breach notification, heavy regulatory fines and the statutory empowerment of data subjects to litigate and seek compensation will start to 'bite' and cause economic and reputational harm to their businesses.

Is there a need for the court to be empowered with greater power, besides issuing fines, to ensure compliance?

In relation to personal data theft by individual and companies, deterrence is a key aspect of the sentencing process, as it will seek to dissuade others from becoming involved in criminality of this nature. The imposition of a fine (the only sentencing power available at present to a criminal court) is insufficient in deterring further criminal activity in this area. Criminal courts need to be empowered so that the full range of sentences that are available to a criminal court—immediate custodial sentences, suspended sentences of imprisonment and community based orders—allow the court to accurately reflect the seriousness of the offending, punish the offender and deter others from committing offences of this nature.

On a corporate level, in relation to the data protection regulatory framework, the increase in regulatory fines in conjunction with the ability of consumers to litigate and seek compensation for breaches of their personal data will no doubt affect a change in due course as to how businesses engage with regulators and consumers, and increase levels of co-operation and transparency.

What impact will the expected introduction in the GDPR of a 'one stop shop' for regulatory supervision have in this area?

As stated above, the GDPR allows the regulators to have more effective powers and sanctions while simultaneously increasing the rights of the consumer. The key is for businesses to appreciate this change of approach and emphasis, and to address it in a constructive manner to ensure their compliance and economic wellbeing.

Ian Whitehurst specialises in criminal and regulatory law with a particular emphasis on commercial fraud, confiscation and cyber related litigation. He is ranked as a leading barrister in all the main professional directories for crime and financial crime.

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor