The Data Protection Act
Ensuring Compliance

Following the fine recently imposed on Sony Computer Entertainment Europe for one of the most serious security breaches the ICO had seen, *Lawyer Monthly* takes a look at the issues raised when attempting to ensure compliance with the Data Protection Act. To this end, we speak to Bridget Treacy, Managing Partner of Hunton & Williams' London office.

Please introduce yourself, your role and your firm.

I lead the UK Privacy and Information Management practice and my practice focuses on all aspects of privacy and information governance for multinational companies, including big data and analytics, cloud computing, cross-border data transfers, behavioural targeting and data breach. My team forms part of the Global Privacy and Data Security practice.

The Information Commissioner's Office (ICO) recently imposed a fine of £250,000 on Sony Computer Entertainment for a serious security breach. (Sony is accused of having out of date security software). What are your opinions on this?

The full facts of the Sony fine are not in the public domain (the ICO's penalty notice is heavily redacted) but the fine sends a clear message that organisations must be proactive about data security. This includes updating security measures to reflect the nature of the data processed, and any known vulnerabilities. The greater an organisation's technological expertise, the better the security should be. The Sony fine also serves as a reminder to data controllers that they remain responsible for data processed on their behalf, even where the processing is carried out by another company in the same group.

What are the main challenges involved in ensuring compliance with The Data Protection Act?

Many businesses still do not take data protection seriously, yet data assets are often the most valuable assets an organisation has. Understanding these assets and the applicable legal framework can yield significant commercial gains. For example, data analytics can help an organisation understand its clients, what they are likely to buy, when and how. Cloud computing offers efficiencies and cost savings. Aggregating data into a single, global database can make a global business more efficient and coordinated. But unless the data protection issues inherent in each of these activities are addressed properly, organisations may find themselves dealing with customer complaints, or regulatory enforcement.

The Data Protection Act requires organisations to satisfy a range of obligations, in addition to data security. Transparency and proportionality are key, but organisations must adopt a structured approach to compliance. It is crucial to know what personal data are held, how that data may be used, and that the data are processed in accordance with the other requirements of the DPA.

Currently, the ICO is able to fine organisations up to £500,000 for a serious breach of the DPA likely to result in harm. Under current proposals for change to the EU data protection framework, failure to comply with data protection laws may result in a fine of up to 2% of an organisation's global turnover.

How can compliance be monitored more effectively?

Given the value of data assets, data protection compliance needs to be seen as a mainstream risk within organisations, not a marginal issue. Senior executive responsibility for data protection can help ensure that the issues are taken seriously. A structured compliance programme with sensible audit checks will help to ensure compliance.

Many data issues have their origin in the design of products or services. It may be impossible to re-engineer a product that breaches data protection requirements, and commercially embarrassing to withdraw a flawed service from the market. Building data protection compliance into product development, termed Privacy by Design, is crucial for data related products (and services). Many successful data businesses have embraced this concept.

How would you like to see legislation amended to better protect data?

Data protection legislation protects individuals' rights, and seeks to strike a balance between those rights and the ability of organisations to use data. Our existing UK regime generally strikes the right balance between these issues, but is somewhat out of date given recent advances in technology, the volumes of data processed, and the way in which data is used. The proposed European data protection Regulation rightly seeks to enhance individuals' rights but currently proposes too many unworkable restrictions on businesses that do not improve data protection.

What are the most common data protection cases you deal with?

Our caseload is extremely varied and reflects the fact that data is a core asset for many businesses, regardless of sector. We advise on the creation and use of new technologies that process data (conducting privacy impact assessments and utilising privacy by design), the use of cloud computing technologies, cookie compliance and behavioural targeting, data analytics and big data, data security breaches and cyber security, regulatory investigations, cross border data transfers (including Binding Corporate Rules), and we help clients build privacy compliance programmes. **LM**

Visit Hunton & Williams' privacy blog at **www.huntonprivacyblog.com**, and its EU data protection regulation tracker at **www.huntonregulationtracker.com**.

Contact Details:

Bridget Treacy
Partner
btreacy@hunton.com

Hunton & Williams
30 St Mary Axe
London EC3A 8EP
Phone: +44 (0)20 7220 5731
Fax: +44 (0)20 7220 5772
www.hunton.com

HUNTON & WILLIAMS