SQUIRE SANDERS

Information Commissioner's Fines – How to Avoid Them

Last month, the Information Commissioner's Office (ICO) imposed its largest fine to date, £325,000, on Brighton & Sussex University Hospitals NHS Trust. Just last week it imposed its second largest, £225,000, levied against Belfast Health & Social Care Trust.

As the ICO has now had the power to fine, up to £500,000 per data protection principle breached, for two years, what lessons can be learned about its priorities from its fines and other regulatory sanctions in that period?

Data Security or Data Breach

The overwhelming majority of the monetary penalties levied have been for failure to keep personal data (and particularly sensitive personal data) secure, leading to data loss or wrongful disclosure of data. This publication will, therefore, concentrate on data security. A subsequent alert will address other enforcement priorities.

Many of the events leading to fines have involved the inadequate security of the organisation itself. A number of fines, however, have been imposed when the security measures (or lack of them) of a contractor hired by a business have been poor.

In the case of the Belfast Trust, the failure lay with the Trust itself in leaving sensitive patient records in a disused hospital. In the case of the Sussex Trust, however, and a number of others, they were fined because they subcontracted work to another organisation, and failed to put an agreement in place with them, or to check their security measures. The Sussex Trust was held responsible when hard disks that should have been destroyed by their contractor were sold on the Internet by the contractor, still containing sensitive personal data.

Many of the fines have been imposed when the data breach occurred because of the wrongful (and often criminal) act of a third party. In the case of the Sussex Trust, its contractor committed a criminal offence. In a number of cases, portable devices containing personal data were stolen from an employees' home or car. None of the cases involved deliberate wrongdoing on the part of the data controller. In one case, personal data became publicly available after a hacking attack on a company's website.

All, however, involve an inadequate approach to data security. The biggest monetary penalties have been imposed when there was an ongoing failure by the data controller. Some, however, have been levied for a single breach, such as faxing or emailing a sensitive report to the wrong fax number or email address.

Avoiding Data Security Breaches

The actions that need to be taken fall into two categories, practical and legal.

Practical Measures

- Identify what personal data and particularly any sensitive personal data you hold. This may be either sensitive within the meaning of the Data Protection Act 1998 (Act), such as information as to a person's race, religion, mental or physical health, sexual life or criminal proceedings, or that an individual would consider sensitive, such as salary or bank details. Check whether you should still be holding the data. If you shouldn't, delete it. If you should, then take security measures appropriate to the degree of sensitivity of the data, and make sure that the measures taken are regularly reviewed, and updated as needed.

- Whenever personal data is stored on or accessed from mobile or portable devices, or transferred across a network, ensure that it is encrypted. In cases where laptops were stolen, the businesses involved could probably have avoided fines if the data held on them had been encrypted.
- Put systems in place to deal with security breaches so that any problem is quickly identified and addressed, and damage to individuals, and the company's reputation, limited to the greatest degree possible, as well as reducing the risk of future breaches.

Legal Measures

- Review all the situations where you use a third party to provide services that will or may involve your contractor in having access to personal data. This can range from outsourcing your payroll, to IT support and maintenance, to the contractor who disposes of your waste paper or electronic records.
- If you do not have written agreements in place with them, put one in place immediately, as not to have one is a breach of the Act. Under the Act, it is the data controller who is responsible for breaches of the Act by its data processors. The Act requires that, as a minimum, a data controller must review (at the outset and ongoing) the security measures its processors take, and have in place with them a written agreement requiring them to take all appropriate security measures to keep the data secure, and only to deal with the data as instructed by the data controller.
- If you have a written agreement with your processor that is two or more years old, it may well need to be revised and updated. Two years ago, the ICO had not then specifically stated that holding significant unencrypted data on portable devices is a breach of the Act. Other amendments may also be appropriate. For example, if the agreement does not incorporate a requirement on the processor to notify the controller immediately if a data breach occurs, this point should be addressed.
- Check whether any personal data may be transferred to or accessed by the processor or a sub-contractor outside the European Economic Area (EEA). If it can, then significant additional contractual protection will usually be mandatory. It may not be immediately obvious to you that data may be accessed outside the EEA, but if, for example, your IT service provider is part of a global group, and/or provides support 24/7, they may well be providing some of that service from outside the EEA. More and more service providers also sub-contract some work to lower cost organisations outside Europe.

Aggravating/Mitigating Circumstances

Fines are most likely to be imposed, and will be largest, if there are repeated breaches, when the data controller has done little or nothing to address previous breaches. The ICO also regards most seriously failures in a company's policies and procedures which indicate that a problem is the result of systemic shortcomings.

On the mitigation side, if, when a data breach occurs, an organisation acts swiftly (the first 24 hours are crucial) to put the problem right and minimise damage and distress to affected individuals, as well as putting its house in order as regards policies, procedures and training, this can make the difference between a fine and lesser regulatory sanctions, as well as minimising the adverse PR consequences for the company.

Guidance From the ICO

The ICO has issued a number of guidance documents in this area. Most recent is *A Practical Guide to IT Security* for small businesses. It has also issued guidance on dealing with data breaches including when such breaches should be notified to the ICO. They can be accessed on the ICO's website at www.ico.gov.uk.

SQUIRE SANDERS

How Can Squire Sanders Help?

Squire Sanders has extensive experience in assisting clients in all aspects of security and data protection. This includes:

- Helping clients to undertake data audits and risk assessments;
- Drafting and assisting clients to implement necessary policies and procedures to keep data secure;
- Providing training on data security and protection to clients and their employees;
- Providing frameworks for clients to assess the data security of their contactors, and drafting and negotiating agreements to address data security, both within Europe and beyond;
- Advising clients in urgently addressing data breaches, some highly sensitive and high profile; including dealing with notification or complaints to the ICO, and advising on mitigation measures.

For more information, advice or assistance in any of the areas mentioned above, contact any of our lawyers in this area listed below.

Contact

Delizia Diaz
T +44 121 222 3383
delizia.diaz@squiresanders.com

Caroline Egan
T +44 121 222 3386
caroline.egan@squiresanders.com

Francesca Fellowes
T +44 113 284 7459
francesca.fellowes@squiresanders.com

Paul Jinks
T: +44 113 284 7234
paul.jinks@squiresanders.com

Ann LaFrance
T: +44 20 7655 1752
ann.lafrance@squiresanders.com

Garfield Smith
T +44 20 7655 1365
garfield.smith@squiresanders.com