SCOTTISHLEGALNEWS
News, Events and Jobs in Scottish Law

Blog: Law Firms beware of the Information Commissioner

Laura Irvine *writes on the importance of complying with the Data Protection Act 1998.*


Laura Irvine

Last month the Information Commissioner's Office (ICO)published an undertaking outlining an agreement it had reached with a small Scottish law firm. The ICO was of the view that the firm had breached the Data Protection Act 1998 (DPA) but rather than taking formal enforcement action, it appears that the firm agreed to take certain steps to ensure future compliance. This highlights the significant obligations that law firms of all sizes have under the DPA to ensure that any personal information they hold is looked after and kept secure.

Breach of the DPA

The law firm asked a third party to collect a DVD from the Procurator Fiscal's office containing CCTV footage of its client who was being prosecuted. The DVD was unencrypted (which may also present issues for COPFS) and the DVD was lost by the third party.

Under the DPA the law firm was the data controller in relation to the DVD. Itwas obliged by the seventh data protection principle to have in place "appropriate organisational measures" to ensure that any personal information it processesis not accidentally lost. The ICO appears to have found that it did not have in place the measures it would expect and so had breached the seventh principle.

In this case the personal information was "sensitive personal data" as it related to the alleged commission of a criminal offence. This data attracts additional protection by the DPA and if compromised, it is generally treated more seriously by the ICO.

Finally if a third party is doing anything with personal data on behalf of a data controller, the data controller retains responsibility for the data and is obliged under the DPA to have a written contract in place telling the third party processer what to do, ensuring that it is maintaining the same standards of data security. Failing to comply with the DPA, the law firm was responsible for the actions of the third party and therefore the loss of the sensitive personal data..

Appropriate Organisational Measures

The ICO investigated the incident and discovered "a number of shortcomings in the organisation's procedures". The law firm undertook to introducethe following "appropriate measures", within three months, and it is clear that these are the measures that the ICO expects organisations that process personal data to have in place in order to comply with the DPA:

- Produce appropriate procedures for the collection of paper and electronic media containing personal and sensitive personal data from third parties;
- Ensure that safeguards are put in place to use encryption where appropriate;
- Implement a Data Protection Policy;
- Make staff aware of that Policy and ensure that they are trained as to how to follow that policy; and
- Ensure that staff responsible for the handling of personal data are given appropriate, specific training upon induction and this training is refreshed annually.

What the ICO could also have done

An undertaking is an informal enforcement tool used by the ICO when it is satisfied that a breach of the DPA has occurred. It is negotiated with the offending party but has no statutory basis and no formal status – although it is publicised on their website and clearly has reputational risks for the organisation concerned.

The ICO could have issued an enforcement notice in this case which is a statutory enforcement tool with teeth – failure to comply is a criminal offence. Finally, if the ICO considered that there had been a serious breach, and that it was "of a kind that was likely to cause substantial damage or substantial distress", then it could have issued a monetary penalty of up to £500,000.

As law firms regularly deal with information which clients expect to remain confidential and which can often fall into the category of sensitive personal data, such as medical information or evidence of a criminal conduct, it is immensely important they are complying with the DPA.

If such data was lost or compromised, the ICO could reasonably demonstrate the potential for substantial damage or substantial distress. If the "appropriate measures" highlighted above as well as the measures required by the other seven data protection principles are not in place, then law firms of any size risk attracting the ICO's attention, alongside reputational damage and the significant penalties that can be imposed. Law firms beware!