What companies need to know about data protection registration when using CCTV

Date : March 6, 2015

In October 2014 the UK data protection regulator, the ICO, published a Code of Practice relating to the use of CCTV on corporate premises. We reported on it here. The ICO have spoken about the *"wider privacy concerns"* of the use of CCTV in the UK.

Using CCTV on a company's premises brings the Data Protection Act 1998 into play. Under the DPA 1998 when a company processes the personal information of members of the public it must put details of the information it collects on a public online register. The register records the way in which the company is using this personal information. There are 33 listed ways in which information can be used. Each company must pick out of the list the ways in which they use data and register that use.

If your company has started using CCTV on its premises and it has not yet registered with the ICO then it must do so immediately. If your company has started using CCTV on its premises but is already registered with the ICO then it may need to update the information that the ICO keeps on its register. You may, for example, be using the CCTV to collect information for *"Crime prevention and prosecution of offenders"* in which case the register should be updated to show this.

Failure to register, or to notify the ICO of changes, is an offence. In 2012 the ICO prosecuted a bar owner in Lancashire for failing to register his premises for use of CCTV equipment. This is a strict liability offence. It does not matter if the failure to notify was accidental. Company directors, secretaries and managers may be prosecuted as well as their companies. The maximum penalty is currently £5,000. Failing to notify can bring not just prosecutions but also the negative publicity that ensues from being publicly named by the ICO.

Once you have registered however that is not the end of the story. You will also need to process information from the CCTV system in accordance with data protection law. In October we explained some of the responsibilities in our alert then and we spoke about the guidelines that the ICO released – *"A Data Protection Code of Practice for Surveillance Cameras"*. You can view that alert here. This is an area where the ICO has already been active. In 2011 for example the ICO took action against a CCTV monitoring service, Internet Eyes, which asked homeworkers to monitor CCTV images from its retail clients. The ICO took action after CCTV footage of a shopper from Internet Eyes was posted on YouTube.

In 2013 the ICO issued an enforcement notice to Hertfordshire Constabulary over its use of ANPR cameras around the town of Royston in Hertfordshire. The scheme was locally known as the *"Ring of Steel"* but the ICO decided that the police's use of these cameras was excessive and unlawful.

Any business thinking of installing CCTV cameras should also do a Privacy Impact Assessment (PIA) in addition to maintaining its ICO registration. The PIA does not have to be filed with the ICO but will be useful in planning the scope of the CCTV system and in explaining how decisions were taken if a complaint is made.

Cordery offer a fixed fee registration and renewal service for ICO notifications. Details are here. Details of Cordery's data protection and privacy practice are here.

Jonathan Armstrong and Patrick O'Kane are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

Patrick O'Kane, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 118 2700