A quick guide to CCTV video and data protection

The Data Protection Act (DPA) ensures that our personal information is not misused by those who collect and process it. Usually, we think of this data as names, addresses, phone numbers, bank or credit card account details and so on. But actually it includes any data that can be used to identify a living person, including still or video images. So video captured by CCTV systems may be covered by the DPA and therefore those responsible for collecting and processing it should operate within the eight principles of data protection.

The eight DPA principles (abridged)

Personal data shall:

- be processed fairly and lawfully
- be obtained only for specified and lawful purposes
- be adequate, relevant and not excessive
- be accurate and kept up to date
- not be kept for longer than is necessary
- be processed in accordance with the rights of data subjects
- be protected against unauthorised or unlawful processing and against accidental loss
- not be transferred outside the EEA without protection for the rights and freedoms of data subjects

The Information Commissioner's Office (ICO) is responsible for promoting and policing the DPA. The CCTV code of practice *'In the picture: A data protection code of practice for surveillance cameras and personal information'* provides advice on good practice for those who operate CCTV systems.

Who is responsible for the system and the data?

The owner of the premises or the director of the business or organisation is the 'data controller' and has responsibility for complying with the DPA. As a 'data processor', Theridion must also process the data in accordance with the DPA. The data controller should establish the reasons for having a CCTV system (e.g. crime prevention, safety, security and property management) and ensure that the system and the data are used only for those purposes.

Who can access the data?

Anyone can make a 'data subject access request', that is a request to view footage or have a copy of images that show himself or herself. However, it should only be provided if the data controller is sure that the request is genuine and that the footage shows only that individual and no-one else. A copy of video footage may also be provided to the police investigating a crime but should not normally be provided to any other third party. A clear record should be kept of all requests for data, whether the request was accepted or refused and to whom any data was provided. The police will normally treat the footage as evidence and process the request formally.

Information for staff, customers and visitors

Signage should be in place so that staff, customers or visitors know that video recording is in use and why. They should also know who to contact if they want to make a data subject access request.

Policy and staff training

As well as complying with the ICO's code of practice, operators should ensure that they incorporate the good practice into their own policies, codes of practice, staff training and systems. Theridion's proprietary *Oggle* remote video system is compliant with the DPA and the ICOs' code of practice, so long as data controllers and operators have a robust policy which is carefully followed.