8 Basic Principles of Data Protection

INTRODUCTION

In 1998, the scope of the Data Protection Act was broadened to enforce 8 principals of good practice regarding the personal data captured about individuals and how this is stored and processed. Personal data included facts and opinions about an individual.

It outlines that any organisation/individual or body who is collecting such information about people must then handle this data in an appropriate manner. ie, that any data collected must be:

- fairly and lawfully processed,
- processed for limited purposes,
- adequate, relevant and not excessive,
- accurate,
- not kept longer than necessary,
- processed in accordance with the data subject's rights,
- secure,
- not transferred to countries without adequate protection.

Inevitably the capturing of personal data by means of a CCTV camera was more readily covered by the Act and closer monitoring of CCTV footage, it's usage and storage became paramount.

For a CCTV system owner, the Act essentially means that:

- they must register their CCTV system with the Information Commissioner,
- they must only take footage that is relevant to their property and it's security,
- they should not keep footage longer than it is necessary for a crime to come to light,
- they should warn individuals when they are in a monitored area,
- they should allow access to the footage to anyone who believes that they have been captured on one of the cameras,
- they should store captured footage securely so that access to it is strictly monitored.

By July 2000, just a few months after the Data Protection Act actually came into force, it became apparent that clearer guidelines were necessary to help CCTV system owners to run and manage their data storage more appropriately. For this reason, a CCTV Code of Practice was written by the Data Protection Commissioner as a guide to good practice for CCTV users.

The full CCTV Code of Practice is also available to download from the Who Is Watching Me website – this was recently updated in 2008.