CCTV and General Data Protection Regulations – Guidance and Points to Note

If you are using CCTV in your business for crime prevention purposes then you need to be aware of the GDPR implications – importantly you need register and pay a fee to the Information Commissioner's Office. There is more on this below under "Register with ICO".

There are a number of steps required to comply with data protection in the operation of CCTV and the Information Commissioner's Office has an online checking tool to help businesses work through the steps towards compliance. This can be found at

https://ico.org.uk/for-organisations/data-protection-self-assessment/cctv-checklist/

We set out below some information on the steps the online tool takes you through:

Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project. It must

- describe the nature, scope and context of the purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Whilst that sounds quite complex, it is a case of working through what you want the CCTV for, why it is necessary, what risks there are to individuals (so how might their privacy be affected, how might data be lost for example) and the measures to mitigate those risks (for example, CCTV not covering any areas where people expect heightened privacy such as toilets or changing facilities; strong passwords for CCTV access, training of staff who operate or have access to the CCTV images).

There is more information and a template DIPA on the NTF website in the GDPR area and detailed guidance on the ICO website.

Register with the IOC

One of the key points is that you will need to register with the ICO – in general if you are only processing data personal data for the administration of your employees such as paying them, paying their PAYE and pensions, and using the personal data of your clients for sales and accounts purposes, you are unlikely to be required to pay a fee to the ICO. However, the use of CCTV for crime prevention purposes will put you into a different category and you will need to pay an annual fee to the ICO office. The fee depends on the number of people the business employs and its annual turnover. It is £40 - £60 for most small to medium sized businesses.

The IOC website has an interactive tool for businesses to use to see whether or not they are required to pay such a fee. This can be found here

https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/

CCTV Policy

The NTF has a template CCTV policy for you to adapt to your own business needs.

Subject Access Request Policy (SAR)

Individuals have the right to obtain from a company confirmation as to whether the company is processing their personal data, a copy of that personal data and various other supplementary information – a request for such information is called a Subject Access Request.

The NTF has a template SAR policy for you to adapt to your own business needs.

Training

You will need to ensure that

- employees operating or with access to the CCTV have training upon its use, security, storage of data, deletion of data, etc
- employees know the disciplinary penalties for misuse of the CCTV system.
- employees are aware of the procedure for a SAR.

Retention

You need to have a policy in place as to how long data will be retained.

There is further information upon data retention in the GDPR area of the NTF website.

Data Quality

The IOC advises that you should select a system which produces high quality, clear images which law enforcement bodies (usually the police) can use to investigate crime.

Data Security

The IOC advises that security precautions should include technical, organisational and physical security and should:

* protect wireless transmission systems from interception.

* restrict the ability to view or make copies of information to appropriate staff.

* have a secure space where footage is stored.

* and that staff should be trained in security procedures

Fair Processing

This includes ensuring that there is signage alerting individuals to the CCTV.

For all the above there is further advice and explanation on the IOC website in the self-assessment guide referred to at the start of this document and found at

https://ico.org.uk/for-organisations/data-protection-self-assessment/cctv-checklist/