Guidance Note on using CCTV in self-catered accommodation

This guidance is aimed at helping PASC Members comply with data protection legislation when using Closed Circuit Television (CCTV). The same principles apply to Automatic Number Plate Recognition and other surveillance technologies. Throughout this guidance note all forms of video surveillance are collectively referred to as CCTV.

CCTV has become more and more complex in recent years; such developments have raised increasing concerns over privacy issues. There are a several consequences if these processes are not taken seriously, from fines for breaking the law, to complaints from individuals leading to losses in business reputation. The Information Commissioner's Office (ICO) is the UK's data protection regulator who individuals can complain to if they feel their data protection rights have been breached.

We recommend that all Members consider the 10 steps outlined in this Guidance Note before using CCTV on their premises to ensure compliance with the law and minimise the risk to your business.

Step 1 - Carry out a Privacy Impact Assessment (PIA)

The law requires that a Privacy Impact Assessment is carried out for any activity that is likely to result in a high risk to individuals. CCTV will pose a risk to individuals which could in some circumstances be considered "high". That means a PIA should be carried out. Carrying out a PIA should therefore be the first step you take before looking to install CCTV or other surveillance systems. If you already have CCTV in place you should look to carry out a PIA retrospectively to show that you have considered the privacy implications of its use and comply with the law. In carrying out a PIA, you will need to consider if the use of CCTV is a necessary and proportionate way of fulfilling the need/purpose you have identified.

PIAs should also be carried out when:

- cameras are added or removed from systems;
- cameras are moved or change position;
- whole or parts of the systems are upgraded; or
- new systems are installed.

Step 2 – Decide your lawful basis for processing

You must have a valid lawful basis in order to process personal data. Personal data is information relating to individuals who can be identified or are identifiable from the information in question. Images captured by CCTV are classed as personal data and data protection laws apply to their use.

Your processing of personal data via the use of CCTV will be unlawful without a valid lawful basis. There are six legal bases, and the most suitable for your business to use for using CCTV is likely to be legitimate interests. Should you choose to rely on legitimate interests, a separate Legitimate Interests Assessment (LIA) will need to be carried out to show you have carried out the necessary balancing test between the rights of individuals and your legitimate interest.

This, like the PIA, will need to be documented to demonstrate your compliance and kept under regular review.

Stephens Scown have created PIA and LIA templates enclosed with this Guidance Note to help you complete Steps 1 and 2 above.

Step 3 – Consider selection and position of cameras

The type of system you choose and the location of it must achieve the purposes for which you are using it. You should not collect more data than you need. Cameras should not be positioned with a view of private areas, e.g., bedrooms, bathrooms, changing rooms etc. The use of CCTV will be much easier to justify in communal or public spaces such as entrances and car parks. Conversely, it will be hard (and sometimes impossible) to justify use inside private living areas of self-catering accommodation.

As mentioned earlier, you should assess through a PIA whether or not a surveillance system is the most appropriate means of achieving your needs and whether less invasive measures can be taken instead.

Step 4 – Ensure the data is kept securely

Recorded material needs to be stored in a way which is secure. This is to make sure that the rights of individuals recorded by CCTV are protected and that the information can be used effectively for its intended purpose.

To do this, you need to carefully choose how information is held and recorded and ensure that access is restricted. You will also need to ensure that the information is secure and where necessary, encrypted. Encryption can provide an effective means to prevent unauthorised access to images processed in a CCTV system. Some CCTV systems store the data onsite (either on a dedicated device or a computer) while others put the data they collect in the cloud, allowing you to access them from the internet. Internet accessible systems are more convenient but will carry more risk from a security perspective.

Recorded images should also only be viewed in a restricted area, such as a designated office, and restricted to only authorised personnel.

Step 5 – Decide on Retention Periods

You will need to set an appropriate retention period for CCTV footage. The retention period should be based upon the purpose for using CCTV in the first place, and how long the recorded information is needed to achieve this purpose. For example, you should only retain information showing criminal activity for as long as it is needed for an investigation by authorities and should not be kept indefinitely.

You will need to have a policy in place setting out the information you hold, what you use it for, and how long you intend to keep it. You should regularly review the data you hold; you cannot keep data forever and individuals have a right to ask for it to be erased in certain circumstances.

Step 6 – Put a CCTV Policy in Place

Staff using the surveillance system or footage should be trained to ensure they comply with the law. In particular, do they know:

- What your policies are for recording and retaining information?
- How to handle the information securely?
- What to do if they receive a request for information, for example, from the police?
- How to recognise a subject access request and what to do if they receive one? (see below for further guidance on this)

A Clear CCTV policy should be put in place to explain the above to staff and training provided where required.

Step 7 – Be aware of Disclosure Risks
You need to be careful not to disclose your CCTV footage to third parties where you are not entitled to do so for example to neighbours, guests, or members of the public without a lawful basis to do so. If information is disclosed where it should not have been, it would be classed as a data breach and may need to be reported to the ICO. If you do not have the correct safeguards and policies in place to prevent unauthorised disclosure, this can lead to complaints and the risk of serious fines.

Any requests for requests for access to CCTV footage must therefore be handled with care and legal advice sought before sharing footage.

Step 8 – Be prepared for Subject Access Requests
Individuals whose information is recorded have a right to request a copy of the information you hold about them. Individuals can make a subject access request for this information which must usually be provided to them within a calendar month.

You should make sure that the design of your surveillance system allows you to easily find and collect personal data in response to subject access requests.
When disclosing CCTV images of individuals, particularly when responding to subject access requests, you need to consider whether the identifying features of any of the other individuals in the image need to be hidden, or 'redacted' and you should consider the technical challenges this poses when selecting an appropriate system.

Step 9 – Let people know you are using CCTV
Signs
You must let people know when they are in an area where a CCTV system is in operation. The most effective way of doing this is by using signs at the entrance of the premises in question that are easily readable and are visible before the individual is captured on camera. CCTV warning signs should indicate that the system is in use and give information about who is operating the cameras, their contact details and the purpose for which CCTV is in use. Once you have stated your purpose on your signs, you cannot then use CCTV for something else, e.g., if you state your purpose is for crime prevention you cannot then use the footage for bringing disciplinary action against staff.

Covert surveillance is not covered by this guidance note and would need a separate PIA due to the privacy risks involved of such activity which should not be undertaken lightly.

Privacy policies
If you are considering using surveillance systems, you will need to make sure all of your privacy policies are up to date and will need to create a CCTV policy if you do not already have one. You will need to make sure you update both your privacy policies with guests and employees.

Step 10 – Register with the ICO
If you are intending to use CCTV, you should register with the ICO first. For more information on whether or not to register with the ICO, please refer to the further guidance note 'Do I need to register with the ICO?'.

Keep it under review
When you have followed the above steps and have set up the surveillance system, you need to make sure it continues to be compliant with the law.

Any documented procedures that you put in place following this Guidance Note should be regularly reviewed and updated if you make changes to the system (for example adding extra cameras or moving them) or your processes change..

In addition to this, you should carry out a review at least once a year to assess the system's effectiveness to ensure that it is still doing what it was intended to do and address any privacy issues that have arisen (for example complaints received, requests for information received) by making modification if necessary.

Other considerations

This Guidance Note only covers the data protection considerations surrounding CCTV operation, you should also consider whether planning permission is needed before installation or if there are any additional employment law issues that need to be considered. These issues are outside the scope of this Guidance Note but further advise can be provided by contacting Stephens Scown using the below contact details.

For more information contact: dataprotection@stephens-scown.co.uk or 01392 210700.