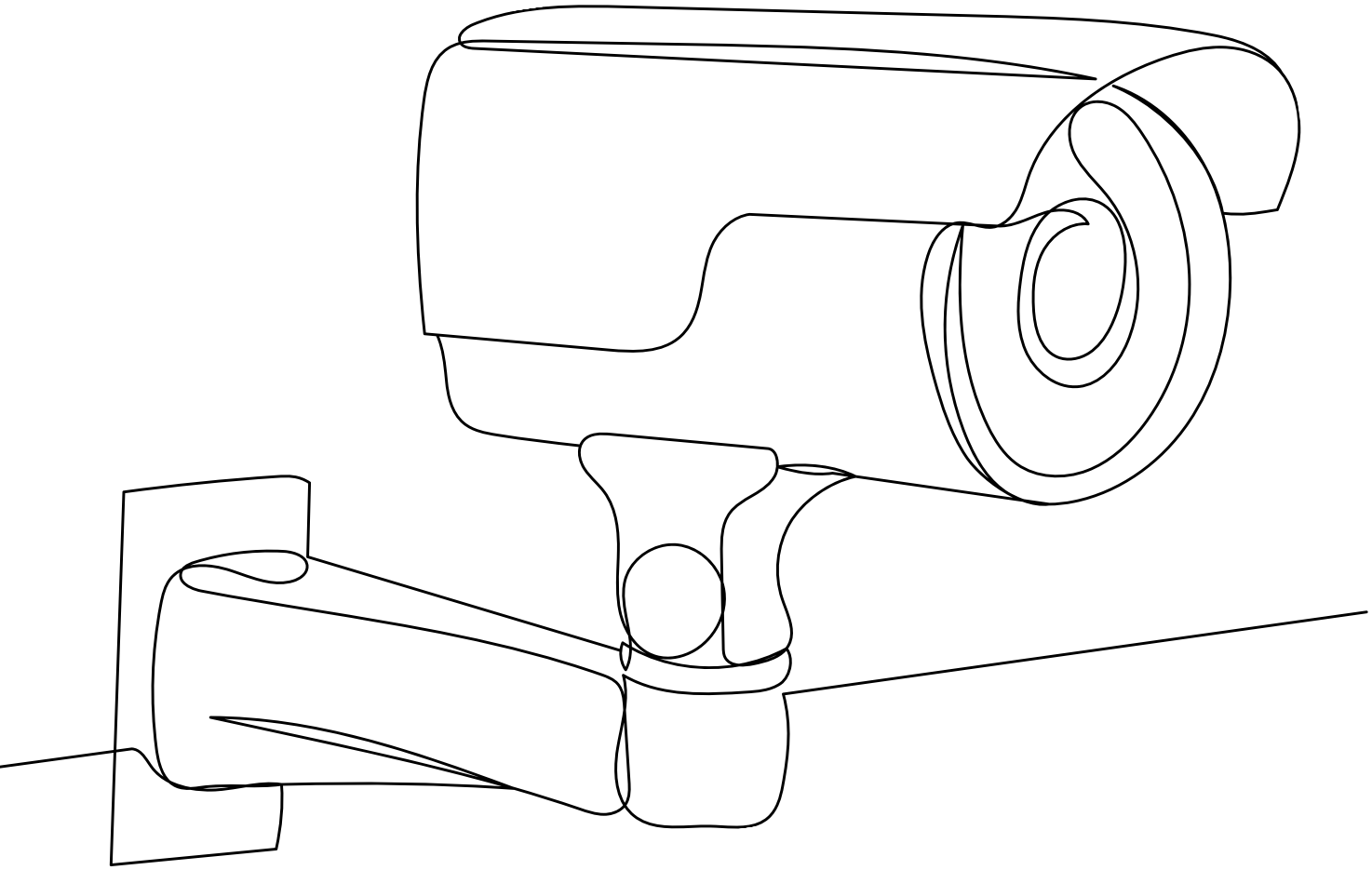
THE OFFICE OF THE
Data Protection Authority

# GUIDANCE: CCTV users



**2023 issue**

# Guidance: CCTV users

## Overview

Closed Circuit Television (CCTV) is used extensively throughout the Bailiwick of Guernsey. This guide is intended to help you use CCTV in accordance with *The Data Protection (Bailiwick of Guernsey) Law, 2017* ('the Law').

*The Data Protection (Bailiwick of Guernsey) Law, 2017* ensures organisations (known in the Law as 'controllers') process personal data fairly and responsibly. Personal data is any information relating to an identified or identifiable, living individual and processing is anything your organisation does with personal data.

If you process personal data, your organisation is legally obliged to maintain an annual registration with us. Our registration guidance provides further information as to when a registration is required and how to create one.

Once you have read this guidance, if you would like further assistance, you can come along to one of our drop-in sessions.

## Who does this guidance apply to?

This guidance is intended for those who are responsible for the operation of CCTV.

Whilst this guidance does **not** apply to the following two groups, you are welcome to use it as an example of good practice to inform your operation of any recording equipment in these contexts:

1. Private householders who collect data for personal, family or household affairs.
2. **Journalists / media outlets** who use recording equipment for journalistic, literary or artistic purposes.

## The Data Protection Principles

The Law is based on seven principles that require you to do the following:

1. Be clear about **how** personal information is used, for what **purpose** and on what **legal basis** (Lawfulness, Fairness and Transparency).
2. Use personal information **only** for specific, explicit and legitimate purposes (Purpose limitation).
3. Collect no more information than is **needed** (Minimisation).
4. Make sure personal information is **accurate and kept up to date** (Accuracy).
5. Keep information for **no longer** than necessary (Storage limitation).
6. Keep information **secure** (Integrity & Confidentiality).
7. Be **responsible and accountable** for how personal information is used (Accountability).

A short checklist to help the controller establish if the principles are being followed is available at the end of this document.

Each principle will now be explained and how it applies to your use of CCTV.

## 1st Principle - Lawfulness, Fairness and Transparency

This principle requires you to have a **valid lawful processing condition** for processing personal data. You are also required to ensure that any personal data you process was obtained without deceiving the person whose data it is and you must make it clear **how** you are going to use their data.

To comply with this principle, you need to identify the purpose and a lawful processing condition for the use of CCTV **before** it is installed. It is essential that your organisation can rely on one of these lawful processing conditions for the use of CCTV to be considered lawful.

Special category data is personal data that is afforded more protection due to its potential to create more or greater risks to a person's rights and significant interests. Images related to alleged criminal offences are special category data. It is essential that you can rely on one of these lawful processing conditions for the use of CCTV to be considered lawful, if you are processing special category data.

The fairness and transparency element of this principle must also be satisfied. To comply with this requirement, the following information needs to be given to individuals at the point of obtaining their images:

- The **identity** of the controller, unless this is self-evident.
- The identity of any **local representative** nominated by the controller.
- The **purposes** for the use of CCTV.
- Any other necessary information to do with the **specific processing** of the information.

Information should be placed in a prominent position to inform the public that they are entering an area where their image is being recorded. It needs to be clear where someone can obtain full details of the processing (your data processing notice or similar), should they wish to do so. This often means the use of signage, traditionally yellow and black. Signs on doors or entrances to buildings should be clear and visible to those entering the building. Signs in outdoor areas should be placed at all points of access.

Please consider other things you may need to think about, such as planning permission to erect signs that may be required from the States of Guernsey Development & Planning Authority.

## 2nd Principle - Purpose Limitation

This principle requires you to only use personal data for the reason or reasons you have told the person you are using it for.

For example, if a night club informs its visitors that CCTV is used to detect public disorder, and the film footage is later used as part of an advertising campaign, then the visitors could claim that the

club has breached this principle as the personal data was used for a different purpose than it was collected for.

Prior to disclosing recordings to any third party, you should establish that that information will only be used for the purpose or purposes for which it was obtained. Where the purpose is for the prevention and detection of crime, then the third parties should be **limited** to:

- Law enforcement agencies
- Courts
- Legal representatives

Where recordings are disclosed to a third party, you should document the following:

- The **date and time** disclosure was made;
- The **name of any third party** to whom disclosure was made;
- The **reason** for disclosure; and
- The **extent** of the information disclosed.

If a controller uses a third party for processing (for example, editing) it is a legal requirement to have a controller/processor contract in place which binds the editing company to certain legal obligations.

## 3rd Principle - Minimisation

This principle requires you to **only** process the minimum amount of personal data necessary to achieve your purpose.

You should give careful consideration to the siting of CCTV cameras so you only record areas that you need to in order meet your purpose of processing.

The purposes the cameras are being used for should be carefully considered and you should ensure the operators are aware of these purposes. Enough information should be recorded to meet the purposes, but they must **not** record information that exceeds the purposes.

It is important that staff operating the equipment are made aware of **why** it is used and that they are well trained, not just about its operation, but also about the implications of collecting data by filming in spaces **not** covered by the scheme.

Many CCTV systems can record sound – but this does not mean that you should. Recording people's conversations is generally considered to be more intrusive than capturing their image. It is unlikely that you need to hear what people say and it is unlikely that you will identify an appropriate lawful processing condition for this type of data collection.

If you have identified a particular need or issue and can evidence that this need can only be addressed by audio recording, you should undertake a Data Protection Impact Assessment ('DPIA').

This will identify additional steps you should take to comply with the Law. This would include making it very clear to people that audio recording is taking place. You should document how you arrived at this decision.

## 4th Principle - Accuracy

This principle requires you to ensure that the personal data you process is accurate and, where relevant, up-to-date.

CCTV recordings could be used as evidence during criminal proceedings or other legal proceedings so it is essential that images recorded are fit for the purpose for which they are intended. If the system uses features such as time references and / or location references, then these must be accurate.

## 5th Principle - Storage Limitation

This principle requires you **not** to keep personal data for longer than you need it.

To decide how long images should be kept, you need to consider the purposes of the processing. If the CCTV is being used in a shop to capture any shoplifting, such incidents are likely to be identified quite quickly so a short retention period (such as 30 days) may be appropriate. If the CCTV is being used to monitor unauthorised access to a remote building, visited only infrequently, a longer retention period may be appropriate. You should document your reason for the decision that you make.

Once the retention period you decided on has passed the data should be erased.

If images or recordings are needed as evidence for legal proceedings or to be kept for other, legitimate reasons, they should be stored in a secure place to which access is controlled. The images and recordings should be destroyed when no longer needed.

## 6th Principle - Integrity and Confidentiality

This principle requires you to keep personal data safe so that it does not get accidently deleted or changed, or seen by someone who is not allowed to see it.

You need to consider the **harm** that individuals could experience due to the lack of appropriate security measures. The nature of the personal data is a significant factor in your assessment of the degree of harm that could be caused.

It is in your interest to avoid making **unauthorised disclosures** of recordings this could cause harm to individuals and reputational damage to you.

Many individuals may feel that CCTV monitors and records them in locations and situations which they consider to be sensitive. For instance, they could be in a doctor's waiting room or even in a retailer's changing room. Individuals could suffer degrees of distress if images are mishandled or if restrictions are not placed on who has access.

Only those staff that need to control the CCTV system for legitimate purposes, for example to position moveable cameras, should be given permission to enable this.

Images and recordings taken from the CCTV system should be stored securely.

Access to images and recordings should be restricted to authorised personnel, for example, a manager or designated member of staff. Viewing of the images should take place in a restricted area. Other employees should not be able to enter when viewing is taking place.

When images or recordings are viewed, you should document the following:

- The date and time of removal of images for viewing;
- The name of the person removing the images;
- The name(s) of the person(s) viewing the images;
- The reason for the viewing;
- The outcome, if any, of the viewing; and
- The date and time images returned to secure place if they are to be retained for evidential purposes.

Prior to disclosing recordings to any third party, you should ensure that the **Lawfulness, Fairness and Transparency** principle is satisfied.

## 7th Principle - Accountability

This principle requires you to be able to demonstrate that you are compliant with the other principles.

This means making sure that you have documented the reasons for making the decisions you did about how you comply with the other principles, for example, what you are using CCTV for, how long you are keeping it, who can view it and so on.

You also need to respond to requests from people who are exercising their rights under the Law. The following link provides further information on Individuals Rights.

In the context of CCTV, it is important to understand the obligations placed on you by section 15 of the Law regarding facilitating any data subject rights request. A person may make a 'data subject access request' to you for a copy of the recording of their image. In certain circumstances you can

refuse these requests. This would most commonly be if the release of the recording would be **likely to prejudice** the purposes of the prevention and detection of crime.

You may wish to designate a member of staff to be responsible for dealing with such requests.

You are expected to take appropriate steps to ensure verification of the identity of someone making a request. This may include requesting a recent photograph.

It is emphasised that subject access requests **cannot** be refused due to the expense incurred for editing and copying. In deciding to use CCTV systems you **must accept the right of individuals** to access their personal data and ensure you have appropriate mechanisms to facilitate these requests.

It is a legal requirement that if you use an editing company, then a controller/processor contract which binds the editing company to certain legal obligations, must be in place.

# CCTV Checklist

The collection and use of images that identify individuals has the potential to impact those individuals. Where a decision is made to install or use equipment, full consideration must be given to all the legal, regulatory and ethical issues which arise.

| | Checked (Date) | By | Date of next review |
|---|---|---|---|
| Personal data, including images, are being collected: Personal data collection | | | |
| We are registered as a controller/processor: Registration | | | |
| Information about the processing of personal data is given to individuals (e.g. clear signage): Informing individuals | | | |
| A lawful processing condition has been identified for the collection and use of the personal data including a clear and specific identified purpose: Lawful processing | | | |
| We only use personal data for the purpose for which it was collected: Purpose limitation | | | |
| We only collect the personal data necessary for the purpose for which it was collected: Minimisation | | | |
| We ensure all personal data are processed and stored securely and are only accessible to authorised personnel: Integrity & Confidentiality | | | |
| We only retain personal data for as long as required for the purpose for which it was collected: Storage limitation | | | |
| We have a procedure in place for responding to requests from individuals, including access to personal data: Accountability | | | |