



The use of CCTV surveillance has become more prominent in recent years, due to the increased sophistication and availability of technology in this area. CCTV has many **legitimate uses** in security, prevention and detection of crime, and health and safety. It can also give rise to **concerns of unreasonable intrusion** into the privacy and data protection rights of individuals and that **excessive monitoring** or surveillance may be taking place.

This guidance is intended to assist people in **understanding what their rights are** in relation to the processing of their personal data by CCTV and what they can expect from data controllers who use CCTV systems.

Where you consider that your rights have been infringed by the use of CCTV, you can [make a complaint](#) to the Data Protection Commission (DPC). There is further information on our [complaint handling process available on the DPC website](#).

### Transparency

You have a right to be provided with **transparent information about the processing** of your personal data. This applies to the recording of your image by means of CCTV. **Clear signs** should be in place to advise people that CCTV recording is taking place in a location, and to outline the purposes for it. The signs should also provide the **contact details** of the relevant data controller or their agent, should you wish to get **more information** or access your personal data.

### Legal Basis - Is Consent Required?

All processing of personal data **requires a legal basis**. One such basis is the consent of the individual; however, this is rarely the appropriate legal basis for the use of CCTV. In many cases, CCTV footage may be recorded based on a **business's legitimate interest** to protect their premises and property from crime or damage, or to ensure the health and safety of staff members and the public. A data controller using a CCTV system should be able to **provide you with an explanation** of the legal basis for processing your personal data on request.

Where a data controller uses CCTV based upon their legitimate interests, they must be in a position to explain to you how they have **justified this based on necessity and proportionality**. If you are not satisfied that their use of CCTV is justified or proportionate in terms of its impact upon you, you have a **right to [make a complaint](#)** to the DPC.

### Access Requests – What Am I Entitled to?

You are **entitled to be informed** about any processing of your personal data that is taking place, and to be **provided with a copy** of your personal data being processed. The information to which you are entitled includes the **identity of the data controller**

and the **purposes** for which they have obtained your personal data. You should also be informed if your data has been **provided to any third parties**.

You are entitled to access your **own personal data only**, and not the personal data (images) of any third parties.

A data controller must provide you with a copy of your data **within one month** of your request, **free of charge**. The controller may extend this period by a further two months, if necessary, taking into account the complexity and number of requests. They can request further information from you as may be necessary to **confirm your identity** and to clarify the date and time that recording took place.

If you are not satisfied with the response that you receive to a request for access, you have the **right to make a complaint** to the Data Protection Commission.

## The Workplace – How Can CCTV Be Used?

The use of CCTV systems is **common in many workplaces** for **security** purposes and to ensure good **health and safety** practices. Employees are entitled to a **reasonable expectation of privacy** in the workplace, however, and the use of CCTV should not have a disproportionate impact on this expectation. In particular, CCTV should **not be employed** in areas where employees **spend their free time unless it can be justified**, for example, based on a need to monitor safety and security. It is generally considered that the threshold for justifying the use of CCTV in breakrooms, changing rooms, and bathroom areas is difficult to meet.

On occasion employers may have recourse to use CCTV footage to **investigate instances** of gross misconduct, negligence, staff discipline, etc. As long as this is done in a **fair and proportionate manner**, in compliance with the principles of data protection, it is likely to constitute lawful processing, as employers have a legitimate interest to protect their premises, employees and members of the public or may be required to process this data to comply with a legal obligation. The data protection rights of employees who are suspected of gross misconduct or other serious disciplinary matters should generally not be considered as presenting a blanket impediment to the use of CCTV by employers in these circumstances.

## Covert Filming

The use of recording mechanisms to obtain data **without an individual's knowledge** is **generally unlawful**. Covert surveillance is normally only permitted on an **exceptional**, case-by-case basis, where the data are kept for the purposes of preventing, detecting, or investigating offences, or apprehending or prosecuting offenders.

## Online Publication of Recordings

If you are aware that your image or recorded footage has been published on a social media platform online, **you can request** that the social media platform used **remove it**.