DOES YOUR COMPANY COMPLY WITH GDPR?

A Complete Guide on UK Data Law

wcctv
WIRELESS CCTV

TABLE OF CONTENTS

1 What is GDPR?

1.1 Why is CCTV Considered Personal Data Under GDPR?

1.2 Am I Responsible For Complying with GDPR?

1.3 Why is it Important For Your CCTV to Comply with GDPR?

2 GDPR Rules and Responsibilities

2.1 Registering Your CCTV

2.2 Data Protection Impact Assessments

2.3 CCTV Location

2.4 Lawful Basis for the Processing of CCTV Data

2.5 Data Transparency

2.6 Data Minimisation

2.7 Storing and Sharing CCTV Footage Safely

2.8 Right to Request CCTV Footage

2.9 CCTV Auditing

2.10 Reporting Potential Data Breaches

WHAT IS GDPR?

GDPR stands for the General Data Protection Regulation, a legal framework that governs how personal data is collected and processed within the UK.

Personal data covers any information that could be used to identify an individual, including their name, phone numbers, photos and other features that could be used online or physically.

THERE ARE 6 GDPR RULES THAT YOU MUST FOLLOW:

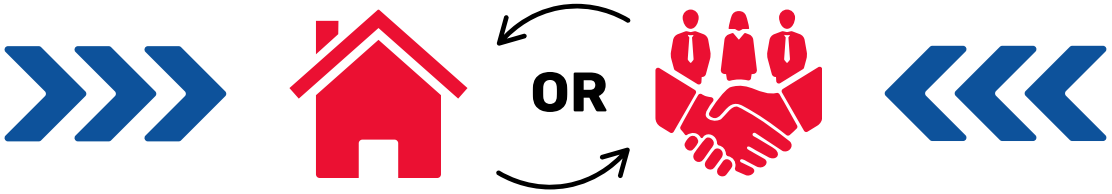
1. Use data fairly, lawfully and transparently
2. Use data for specified purposes
3. Limit the amount of data collected
4. Ensure data is accurate and up to date
5. Keep data for no longer than necessary
6. Keep data secure

WHAT IS GDPR?

WHY IS CCTV CONSIDERED PERSONAL DATA UNDER GDPR?

Where CCTV can capture photo and video that could identify individuals, this is subject to GDPR, just like any other data considered to fall within this law. This also includes any audio.

In all instances, whether it is for domestic use or for business purposes, if your CCTV falls within the above statement, you need to be vigilant with the laws surrounding GDPR.



AM I RESPONSIBLE FOR COMPLYING WITH GDPR?

CCTV controllers are considered as those who have control over how and why data is being processed, placing them as the individuals responsible for ensuring GDPR compliance.

Those holding this responsibility will be expected to manage the compliance for this.

However, even if you are not considered a controller, it is still important to understand the compliance rules surrounding CCTV with GDPR.

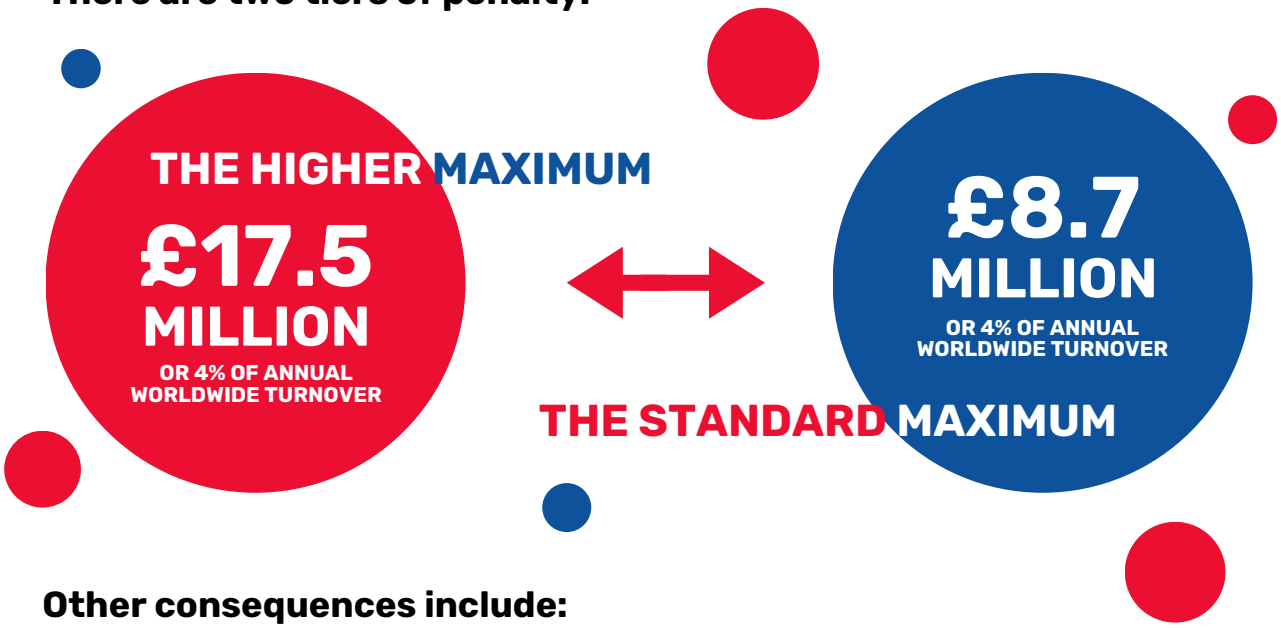
WHAT IS GDPR?

WHY IS IT IMPORTANT FOR YOUR CCTV TO COMPLY WITH GDPR?

Complying with GDPR is important in protecting individual's personal data, any breaches could place that information at risk and lead you to face consequences from this.

The Information Commissioner has the power to implement monetary penalties for the infringement of Part 3 of the Data Protection Act - Law Enforcement Processing.

There are two tiers of penalty:



Other consequences include:

- Reputational Damage
- Loss of Business, Customers and Domestic Relationships
- Legal Action From Data Subjects

GDPR RULES AND RESPONSIBILITIES

In this section we provide the various rules and responsibilities for all individuals considering CCTV or those currently using it.

REGISTERING YOUR CCTV

Initially, you need to **register your CCTV with the Information Commissioner's Office (ICO).**

This is **not** required for domestic use if the view is only of your home or garden, however, in all other instances where you are capturing video outside your property boundary, you must **inform** the ICO.

For businesses, you must register your system, especially those with any external CCTV systems as they will capture public spaces and personal information from individuals.

For domestic use, you cannot directly focus on another person's home or home boundary as this could be considered as an invasion of privacy.

REGISTER NOW

GDPR RULES AND RESPONSIBILITIES

DATA PROTECTION IMPACT ASSESSMENTS

Following registration, a Data Protection Impact Assessment (DPIA) may need to be completed in some instances before any processing begins.

It is a useful tool to help identify the impact of CCTV on people and how to reduce risks present.

You must do a DPIA when data processing is likely to result in a high risk to the rights and freedoms of individuals.

The term **'high risk'** within this context represents the potential for any significant physical, material or non-material harm to individuals. ICO provide the following list of operations where alone or where some are combined require a DPIA automatically:

- Innovative Technology
- Denial of Service
- Large-scale Profiling
- Biometrics
- Genetic Data
- Data Matching
- Invisible Processing
- Tracking
- Risk of Physical Harm
- Targeting of Children or Other Vulnerable Individuals

GDPR RULES AND RESPONSIBILITIES

CCTV LOCATION

Due to privacy laws, there are limitations with where CCTV cameras can be set up.

Locations considered to be private areas such as toilets, changing rooms, and places where say employees expect privacy should **not** have CCTV set-up there.

LAWFUL BASIS FOR THE PROCESSING OF CCTV DATA

For businesses, they must have a **lawful basis** for the processing of CCTV data and the purpose it was intended for must be the only purpose in which the CCTV data is processed based on.

A lawful basis will often be provided based on legitimate interest. This includes:

Ensure Safety and Security

Protect Assets

Monitor Unlawful Activity

Protect Staff

GDPR RULES AND RESPONSIBILITIES

DATA TRANSPARENCY

For both businesses and domestic CCTV where it covers outside the property boundaries, you must be transparent that CCTV is present and in operation, providing clear signage to indicate this.

There are several rules surrounding signage to ensure individuals are informed correctly with privacy laws considered:

Signs Must be Clearly Visible:

They need to be readable and clearly indicate that CCTV is in operation, making sure the sign suits the location it is in. For example, an A4 sign for internal usage and A3 for external usage.

Signs Should Include Details:

They must include details such as, a mailing address, website, or phone number as a point of contact.

Signs Should Explain the System's Purpose:

You need to include who is responsible for the CCTV. This could be a specific person or organisation.

Signs Should Explain the System's Purpose:

Due to privacy laws, individuals must be informed when their personal information is being collected.

GDPR RULES AND RESPONSIBILITIES

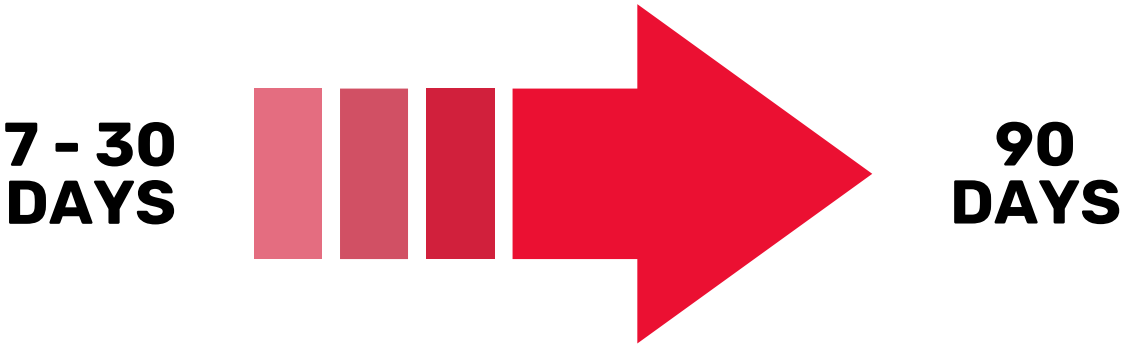
DATA MINIMISATION

CCTV footage should only be collected and retained for as long as necessary to achieve the purpose it was stated for.

If you hold onto CCTV for longer than deemed necessary, you could be found to be in breach of the rule on data minimisation under GDPR.

The term **'as long as necessary'** is subject depending on the data collection reasoning, however, this should be considered before you begin processing.

The most common retention period tends to be 7 to 30 days, but this can go up to 90 days in higher-risk environments.



GDPR RULES AND RESPONSIBILITIES

STORING AND SHARING CCTV FOOTAGE SAFELY

When storing CCTV footage, appropriate security measures should be implemented to protect CCTV footage from unauthorised access, loss, or destruction.

These measures include encryption, permission-based access controls, and safe storage systems.

Access of such footage should be restricted and there needs to be clear rules on who can access it and why, ensuring that when it is shared to others within a business that personal data is redacted and hidden, except the data subject.

For domestic CCTV, there are restrictions on sharing also. You should avoid sharing any footage publicly online and only share in cases where necessary such as, for security, legal reasons, obtaining consent and supporting the police.

In all cases where a criminal offence has been captured, you must comply with:

Article 10 of GDPR

GDPR RULES AND RESPONSIBILITIES

RIGHT TO REQUEST CCTV FOOTAGE

You must provide CCTV footage to anyone who requests it under GDPR.

As a business, you must respond **within one calendar month** of the data subject access request (**DSAR**), however, this can be extended by a further two months if the request is complex or involves a large amount of data. When extending, you must communicate this to the individual who has requested it within **the first month.**

Whereas, with domestic CCTV, where there is a request you must do this within **40 days** and you can charge them up to a £10 administrative fee for doing so.

Below provides a step-by-step guide on the best way to respond to a DSAR:

1. Verify the Identity of the Data Subject
2. Clarify the Request
3. Check if the Requester's Data is Being Processed
4. Inspect, Collect, and Package the Data
5. Provide the Data Subject with Access to their Personal Data
6. If the Request was Received by Email, You Can Send the Information by Email if the Requester Agrees
7. Make Sure the Requester Can Understand the Information
8. Be Transparent in Your Response

GDPR RULES AND RESPONSIBILITIES

CCTV AUDITTING

Legal requirements can change and GDPR law could be altered, therefore you need to keep aware of any changes and audit your **CCTV systems** regularly. For businesses, it is recommended you appoint a Data Protection Officer to do this.

You will need to assess your compliance and evaluate your practices against the GDPR principles to ensure your CCTV system still meets expectations.

If any changes are required, implement them as quickly as possible to avoid breaching any laws.

REPORTING POTENTIAL DATA BREACHES

Where data breaches may have occurred you must inform the ICO.

This can be completed online via the ICO website with the Data Security and Protection Reporting tool, through their webchat or by phone. However, whichever method you decide upon it needs to be completed within **72 hours** and should include the following information:

What happened and when	Individuals and personal data concerned	Your risk assessment	How the breach was contained

WCCTV: MARKET-LEADING CCTV EXPERTS

WCCTV is the UK's leading supplier of portable, managed CCTV cameras for a range of business sectors with multiple crime prevention and investigation applications.

Our mission is to detect, deter and provide digital evidence of crimes by supplying the highest quality surveillance technology backed by a comprehensive service and connectivity package.

With over **20-years experience in security solutions**, we are knowledgeable in all relevant laws and make sure we support you as best as we can in complying with GDPR.