

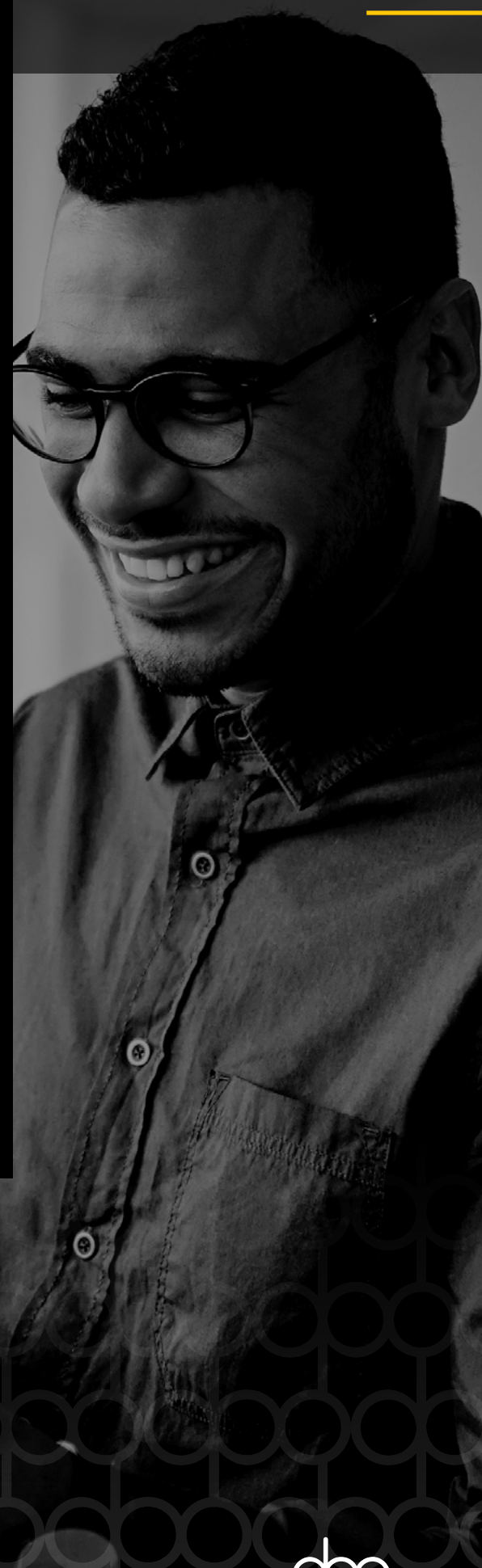
LOOKING THROUGH THE LENS

A DATA PROTECTION
GUIDE TO USING CCTV



CONTENTS

CONTENTS	2
1. ABOUT THE DPO CENTRE	3
2. INTRODUCTION	4
3. DATA PROTECTION AND CCTV	5
4. DATA SUBJECT ACCESS REQUESTS (DSARs)	8
5. ENCRYPTION AND SECURITY	10
6. RETENTION	11
APPENDIX A: INFORMATION TO BE INCLUDED IN A CCTV POLICY	12
APPENDIX B: COMPLIANCE CHECKLIST	13
HOW CAN THE DPO CENTRE HELP?	14



1. ABOUT THE DPO CENTRE



The DPO Centre is a specialist data protection and compliance consultancy, providing data protection related services to over 400 clients from a wide variety of sectors, ranging from commercial, financial services, tech, health, education and 3rd sector organisations.

Formed in July 2017, The DPO Centre delivers consultancy, gap analysis and staff training services, alongside our core business of providing outsourced Data Protection Officers (DPOs). These services are provided on a 'fractional' basis, so range from one to eight days per month, dependent on the appropriate level of need.

Further information on the company, staff and our services can be found on our [website](http://www.dpocentre.com).



2. INTRODUCTION



Closed-circuit television (CCTV) has been in use in the UK since 1960. It was first installed into Trafalgar Square to ensure the safety and security of the Thai Royal Family when they visited the UK. A year later, the country's first surveillance system was implemented to enhance London's railway system.

Since the inception of CCTV within the UK, its use has increased year on year. The UK was once crowned the country with most CCTV cameras per capita in the world, however, other countries such as China, Germany, and the USA now top the charts.

CCTV captures audio and visual recordings ('images') of individuals. It is used in both public and private settings and is therefore impacted by the Data Protection Act 2018 ('DPA').

This guide aims to help you understand the requirements under the DPA when implementing CCTV for domestic and workplace purposes and includes a helpful checklist that can be used to assess the current compliance level of your CCTV set-up.

3. DATA PROTECTION AND CCTV

3.1 ARE CCTV IMAGES PERSONAL DATA?

CCTV images fall under the category of personal data as the images and recordings can identify individuals, either *directly* from recording an individual or *indirectly* through identifiers such as car license plates. As CCTV is classified as a category of personal data, its use falls under the scope of the DPA. However, different rules apply depending on whether it is used in public or private settings as will be highlighted below.

3.2 WHEN DOES DATA PROTECTION LAW APPLY TO CCTV?

CCTV can be used in domestic settings and by organisations – public, private and third sector companies (e.g. charities and not-for-profit organisations). The DPA affects both categories and due care and consideration needs to be applied.

- 3.2.1 Domestic (Private) Setting

CCTV can be used within your home to ensure you feel safe and secure and to protect yourself but, at the same time, you have to respect other people's privacy.

The set-up of CCTV around your home can cause issues depending on what is captured. If the CCTV only captures images within your property (e.g. your garden) and for your own use, the DPA will not apply. However, if the CCTV captures images of people outside your boundary, (e.g. your neighbour's property and gardens or a public area) then the DPA will apply. This also applies to door bells that have cameras installed on them which can record images outside your boundary (e.g. Ring).

The UK data protection regulator, The Information Commissioner's Office (ICO), has produced further guidance and information to help you understand the requirements when using CCTV in domestic purposes which you can find [here](#).



3. DATA PROTECTION AND CCTV CONT...

- 3.2.2 Organisations

If you install and set up CCTV on your premises which can record individuals, you are deemed a “data controller” as you have determined the means and purposes of why CCTV is needed and hold ownership of the data. A third party company may be able to help install the system and provide support with other aspects (e.g. remote support and help with technical aspects of the system) without becoming either a “data processor” or “data controller”. However, if other organisations either monitor or maintain the system for you, they will become data processors and therefore have visibility of the CCTV footage. Therefore, your organisation, as the data controller, should always ensure that there is a compliant agreement in place with the third-party company which reflects the relationship.

As well as the set-up of CCTV cameras, there are other considerations under the DPA that need to be addressed:

1. Have you installed the appropriate signage required for CCTV where needed?

Signs should:

- Be located at the entrance to the area under surveillance
- Be placed within the area under surveillance
- Be clearly visible and easy to read
- Contain details of the organisation controlling the system (if this is not obvious)
- State the purpose for using the CCTV system
- Provide contact details of the organisation operating the system

SIGNAGE EXAMPLE:

“24-hour CCTV is operated by The DPO Centre on this premises for the purposes of safety, security and crime prevention. For more information, please call +44 (0)203 797 1289.”

2. Have you identified who is responsible for the CCTV whilst in operation?

For example:

- Store Manager
- Security Manager
- A third-party contractor

3. Have you implemented a CCTV policy?

Details of what a CCTV policy should include can be found in Appendix A

4. Are your employees trained on the use of CCTV and its purposes as part of their data protection training and awareness? Do they understand the process to deal with a Data Subject Access Request?

The above are examples of what is needed to be taken into consideration due to the obligations imposed on a data controller as per the principles of the DPA, particularly the Accountability principle.

3. DATA PROTECTION AND CCTV CONT...

3.3 INFORMATION COMMISSIONER'S OFFICE (ICO) CHECKLIST

The ICO - the UK supervisory authority for data protection - recommends that organisations intending to install CCTV should carry out an assessment before doing so. The reason for this is, again, to ensure all organisations are demonstrating compliance with the DPA to maintain the safety and security of personal data at all times.

The ICO can carry out an inspection and audit on your CCTV practices to determine your level of compliance and where changes will need to be made.

You can find a sample checklist in Appendix B.

3.4 FINES

Fines under the DPA now follow the two-tiered structure under the General Data Protection Regulation (GDPR) 2016. Fines for the misuse of CCTV fall under the higher tiered fines of 4% annual turnover or €20 Million (£17 Million), whichever is greater.

In April 2019, the ICO fined a TV production company who were filming at a hospital without the Trust's permission. They were fined £120,000 because patients were being filmed without their sufficient consent, as well as there being a lack of information and clear notices, [find out more here](#).

Ultimately, the case was heard under the previous DPA 1998 where the maximum financial penalty was £500,000. However, if the case had been heard under the new DPA 2018, the fine could have been substantially higher.

More recently, in January 2021, a German state Data Protection Authority imposed a much larger fine under the GDPR on an electronics retailer for using video surveillance unlawfully, resulting in them receiving a fine of €10.4 million.



4. DATA SUBJECT ACCESS REQUESTS (DSARs)

4.1 CONSIDERATIONS

We have previously talked about DSARs in a whitepaper titled “Handling Data Subject Access Requests (DSARs)” which elaborated on the rights an individual (data subject) has regarding their personal data, how they can make a request, and the procedures that have to be followed.

Data subjects can make requests regarding access to images and recordings made on a CCTV system. These requests can be made to any organisation a data subject believes has captured them on CCTV: a school; hospital; local council; their employers; and so on.

When a DSAR for CCTV is received, you must ensure the requestor is verified through the use of ID documentation (e.g. a copy of a driver’s license, a passport etc.) and the time and date ranges of the CCTV images. You should also ask how they would like the images to be shared with them.

It is vital you confirm the time and date ranges of the CCTV images due to the principle of Data Minimisation. You are able to refuse requests which are unreasonable and/or disproportionate to the amount of data likely to be available, such as: “please provide all images of me on your CCTV system.”

Individuals are only entitled to copies of their images. If other individuals’ images are also contained within the footage, you will need to make the decision whether to give them a copy of those individuals’ images. This decision will depend on whether they are likely to be able to identify those individuals and whether those individuals could potentially suffer harm from having their images disclosed to the applicant. Where it is deemed that harm could be suffered, you should either use technology to mask the third party or, where this would prove to be

unfeasible, refuse the request. You should note that the ICO may well challenge you on what is considered unfeasible so the presumption should be to provide the footage unless you can clearly demonstrate the unfeasibility.

4.2 POLICE REQUESTS

As mentioned above, CCTV is in place to ensure your safety and security but also to help with the prevention and detection of crime. Please note, the police may also make requests for CCTV footage to help locate missing people. This means whether you use CCTV for a domestic or organisational purpose, the police can request copies of CCTV footage.

If you refuse to comply with a police request for CCTV, they may very well issue you with a search warrant.

Any requests for CCTV footage should be made by an official notice signed by the police. If you feel uncertain about the authenticity of the request, you should clarify this by contacting the relevant authority directly.

4. DATA SUBJECT ACCESS REQUESTS (DSARs) CONT...

4.3 SHARING/PROVIDING COPIES

Ideally you should send the images electronically. However, where this is not possible, you can use a USB stick to download and send the images. The requestor may ask you to send the images through either post or email and you should comply with their request. If the requestor has specified that they would prefer the images to be sent via email, you must ensure the images are saved securely and encrypted with password protection. The ICO recommends the password protected folder and password are sent in two separate emails.

If the requestor has asked for the images to be sent on a CD/DVD or other media such as a USB memory device, it is recommended that the CD/DVD/USB device are all password protected and encrypted. You should ideally send the password via email and double check the correct email address is used. If the use of an encrypted CD/DVD is not possible due to the system being used not being able to read encrypted disks, you should communicate this to the requestor and suggest alternatives, such as using a normal CD/DVD and sending it via recorded delivery, or request they come onto your premises and look at the images in person.



5. ENCRYPTION AND SECURITY



It is recommended that if your CCTV system allows for wireless communication, signals should have encryption. This follows the principle of Data Security.

Through the enhancement and development of certain CCTV systems, there is now the ability to stream and transmit CCTV images through the internet so you can view them remotely. It is recommended these signals are also encrypted to ensure they are not compromised through interception. Most new systems can enable encryption to prevent theft and interception, but having additional layers of access through the use of a username and secure password can also help.

Some CCTV systems allow for live footage to be accessed via mobile phone apps. Where this is the case, access to these apps should be limited to only those individuals within your organisation for which it is completely necessary. If individuals use their personal devices to access the footage, as opposed to a company device, organisations must ensure that they have an effective Bring Your Own Device ('BYOD') policy in place which covers this access, and that this policy is being adhered to by staff.

Another area of consideration is the database/system that holds the CCTV images and where these are kept. These are vulnerable to theft and damage so you should carefully consider where the database/system is kept and what technical and organisational security measures you put into place. For organisations, this could mean keeping them in a locked and secure room with access controls, and for a domestic user you should ensure your surroundings are safe, and that doors and windows are kept shut, locked and curtains closed at night.

6. RETENTION



When you install a CCTV system you must decide how long you are going to keep the images before deleting them. This limit must be clearly defined and not simply be until the system runs out of recording space. Most organisations keep images for 30 days before deleting, however, you may have legitimate reasons to either keep the data longer or shorter than that. Whatever you decide, the retention period must be documented and justifiable. If you are able to find an image that has been requested as part of a DSAR, within the time frames requested and before the overriding date, it is recommended you make a copy of this and save it to a safe, secure computer file and ensure it is only accessible to those within your organisation who need access to it. This should all be reflected within your DSAR policy and procedure.

“Most organisations keep images for **30 days** before deleting...”

APPENDIX A: INFORMATION TO BE INCLUDED IN A CCTV POLICY

Below is a list of the types of information that should be included in an effective CCTV policy. Your CCTV policy should be made easily accessible for staff and you should ensure that they read, understand, and follow this policy whenever they deal with CCTV images.

1. Overview

- Name of the organisation who owns the system
- Name of person(s) within that organisation who is/are responsible for operating the system and ensuring compliance with the CCTV policy

2. The System

- Number of cameras that are part of the system
- Where the cameras are located
- Details of the signage in place

3. Purpose of the System

- Outline of the main purposes of the system e.g. crime prevention
- Details of how the system will achieve the stated purposes e.g. act as a deterrent
- Details of what the system will not be used for e.g. for automated decision making, to publish images online
- Information regarding the circumstances in which covert recording may take place e.g. when there is reasonable cause to suspect that unauthorised or illegal activity is taking place and informing the individual about the recording is likely to prejudice the objective of making the recording

4. Monitoring of Images

- When recording will take place
- Where recordings are monitored from
- Who has authorisation to access the recordings and when
- How unauthorised access will be dealt with

5. Staff

- Steps taken to ensure that staff are aware of how to deal with CCTV recordings
- Details of training provision for staff

6. Recording

- Mode of recording e.g. time lapse, real time
- Retention period
- Erasure/disposal process of data and hard drives

7. Access to Images

- Details of the staff who have access to the recordings
- Confirm existence of an Access Log to be filled out every time an individual accesses any recordings
- Details of the circumstances in which a third party may access the recordings and the procedure for doing so e.g. for a police investigation, for a DSAR

8. Complaints

- Where any complaints about CCTV recording should be sent to

9. Data Breach

- Procedure for dealing with a data breach

10. Compliance Monitoring

- Plan for regular reviews of the CCTV policy
- Plan for regular review of the procedures listed in the CCTV policy

APPENDIX B: COMPLIANCE CHECKLIST

These questions assess how well your organisation complies with the requirements on CCTV contained in the DPA:

- Have you carried out a Data Protection Impact Assessment for CCTV?
- Have you paid the relevant data protection fee?
- Have you implemented CCTV policies and procedures?
- Is clear signage on display and available where appropriate?
- Have you implemented a procedure on how to respond to data subject access requests (DSARs) for CCTV?
- Have you ensured you have an appropriate retention period for CCTV images?
- Have you ensured the CCTV images are of a high quality and clear?
- Are CCTV images securely stored with limited access?
- Have you implemented CCTV awareness training to all staff?

HOW CAN THE DPO CENTRE HELP?


The DPO Centre is an organisation consisting of a team of full-time and permanently employed DPOs located throughout the UK. Every member of this team is an experienced DPO who is knowledgeable and highly adaptable, so can deliver the exact level of support required and in the precise manner required.

This may be to assist you with one-off projects, such as a data protection audit or a complex DSAR request, or to provide support conducting DPIAs. Furthermore we can provide interim support to cover sickness, maternity and employment gaps and can deliver ongoing assistance, as your designated DPO, taking ownership of the day-to-day responsibility for the role, delivered based on the exact level of resource required to meet your evolving needs.

To find out more about our service visit:-

 www.dpocentre.com

 hello@dpocentre.com

 +44 (0)203 797 1289





Head Office

The DPO Centre Ltd
50 Liverpool Street
London EC2M 7PR

Registered Office

Suffolk Enterprise Centre
Felaw Street
Ipswich IP2 8SJ

Dublin Office (Europe)

Alexandra House
3 Ballsbridge Park
Dublin D04 C7H2

Contact Us

+44 (0)203 797 1289
hello@dpocentre.com
www.dpocentre.com 