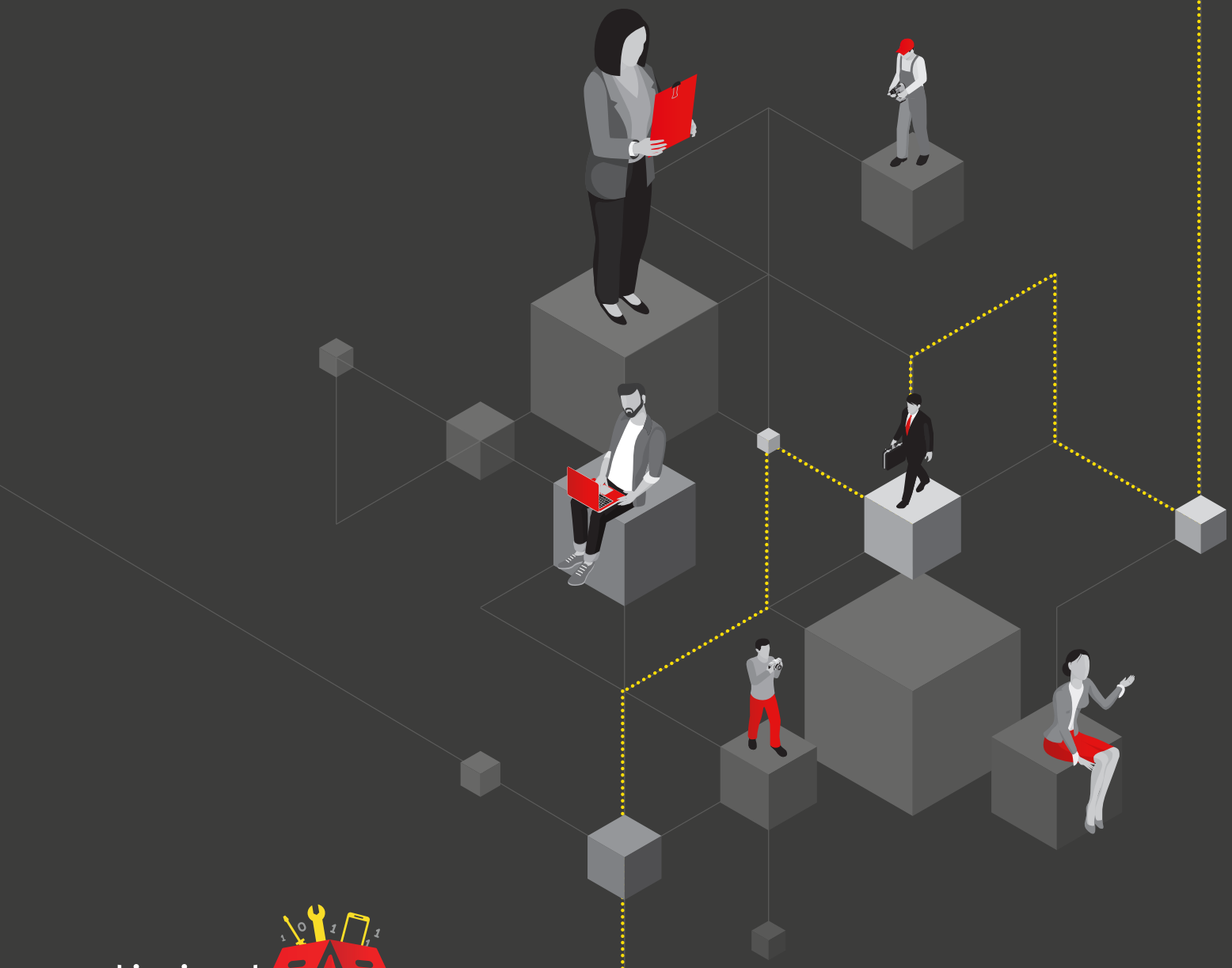
ORGANISATIONS

# SURVEILLANCE & CCTV



digital TOOLKIT

Guidance for Organisations

This document is purely for guidance and does not constitute legal advice or legal analysis. It is intended as a starting point only, and organisations may need to seek independent legal advice when renewing, enhancing or developing their own processes and procedures or for specific legal issues and/or questions.

JOIC
JERSEY OFFICE OF THE INFORMATION COMMISSIONER

WWW.JERSEYOIC.ORG

CCTV is the most privacy intrusive form of data processing undertaken presenting the greatest risk to data subjects.

- CCTV should be used **only** to address real and serious threats to individual health and safety or the protection of property;
- CCTV should be used **only** as a last resort, when other less intrusive approaches have failed.

It is important to take every reasonable measure to limit the collection of personal data from innocent people and to destroy it when it is no longer required for the original purpose.

Disclosure of video images can cause mental distress, loss of dignity, and loss of rights and freedoms for innocent people.

The awareness of being filmed by a camera will likely alter the behaviour of individuals and can cause discomfort or stress. In any case, the mere existence of the camera will undermine personal freedom.

# CCTV use by Businesses, Organisations and Public Authorities

The collection, use, disclosure and retention of personal data, including images, film footage and voice recordings, are all subject to the requirements of the Data Protection (Jersey) Law 2018 (the DPJL).

Before installing a CCTV system or continuing with an existing CCTV surveillance system the following questions will help you to determine whether you are acting in compliance with the law.

You may need to conduct a 'Data Protection Impact Assessment' if there is the potential that the proposed CCTV constitutes high risk. You should document why CCTV is necessary.

## Lawful purpose

What is the LAWFUL PURPOSE for the collection of CCTV images? What are you trying to observe taking place and why?

- Clarity of lawful purpose is essential as it ensures everyone understands what and why you are 'collecting' identifiable personal information;
- Is the CCTV system to be used for security purposes only or are you collecting the personal information for more than one purpose? Can you justify the other purpose(s)?
- It is essential that these purposes are identified at the outset and before any processing takes place;
- Is the personal data captured only to be used for the stated original purpose? For example, if you tell employees that you are installing CCTV to prevent thefts, you cannot then use the footage for another reason (to monitor employee attendance, for example).

# Proportionality

- What are you trying to observe taking place and why?
- Is there a reasonable prospect that CCTV will address the issue/concern? (NB 'We hope it might work' is not good enough. You must have concrete evidence of a real concern or issue and clarity that the installation of CCTV will assist in addressing that issue. It must be more than mere speculation that it 'might' help or that you want to install it 'just in case'. Only realistic threats to health and safety and the protection of property will likely warrant intrusive video surveillance, with few exceptions.);
- Does the threat to property/health and safety etc. outweigh the risks posed by CCTV to the privacy of data subjects?
- Is there any less privacy-intrusive alternative other than using a surveillance system? Have you tried these less intrusive methods and have they failed? Can you evidence this?
- Have you sought out the concerns of the people affected and addressed them?
- Have you carried out a Data Protection Impact Assessment to help you answer these questions?

# Retention & security

- Are you keeping the images recorded only for as long as absolutely required for your purposes?
- Can you delete any unnecessary footage at the earliest opportunity? You must have access to the relevant technology to do this;
- What physical security measures are in place to prevent hacking or loss of footage?
- How are you restricting access to the footage within your organisation? Who has access to it and why? Access should be restricted to those who need to see the information – it should not be available to every individual within the organisation, for example;
- If the States of Jersey Police or insurance companies request copies of your recording ensure they provide you with an authority form and keep a copy of what you send and keep it safe until the conclusion of any investigation.

# Notification and transparency

- Are you notifying everyone whose data is collected?
- Do you have proper signs containing all of the necessary information?

**A CCTV notice must**

→ *Be clear, visible and easy to understand. If you have a large proportion of your workforce whose first language is not English, you may wish to consider making it available in the relevant additional language(s);*

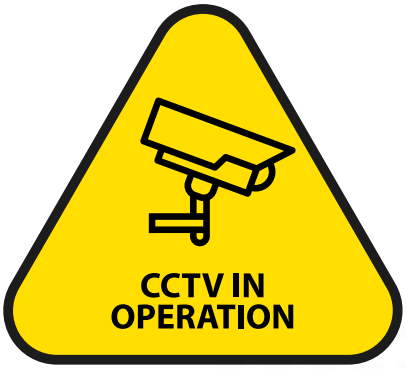
→ *Contain details of the purpose of the surveillance and who to contact about if anyone has any concerns;*

→ *Include contact details such as website address, telephone number or email address.*

- Do you have the relevant policies and procedures available to view?

→ *Privacy Policy* → *Data Protection Policy* → *Retention Policy*

*(Please note: This list is for indication purposes only)*



# Subject access rights

- Are you able to respond to subject access requests? Requests for information by individuals as specified with the DPJL. You must be able to provide data subjects with access to their own information without disclosing that of others;
- Do you have ability to provide an individual with a copy of their own information while deleting or blurring the images of others to prevent identification? This technology may be expensive but is required if you are going to be able to comply with the DPJL unless you can provide that information in another intelligible way.

If, having completed a Data Protection Impact Assessment and documented your decision making you decide that the threat to property/health and safety etc. outweighs the risks to the rights and freedoms of individuals and you install a surveillance system you should ensure that:

- The cameras are not installed in places where people are expected to enjoy privacy, such as inside a changing room/toilet area;
- The surveillance system (both the physical hardware and the images captured) is protected and secure from vandalism or unlawful access;
- The people affected are explicitly informed that they are under surveillance via CCTV, the purpose of surveillance and the means to raise an enquiry;
- The personal data collected by the surveillance system is deleted as soon as practicable when the purpose of the surveillance is completed;
- The effectiveness of the safeguards and procedures for the surveillance system is regularly reviewed.

## FYI

The DPJL in considering the sharing of CCTV images or footage is very clear about 3rd party images

If the supplying of information under Article 28 (4) requires the disclosing of information relating to another individual who can be identified from that information, the controller is not obliged to enable such information to be supplied unless –

(a) the other individual has consented to the disclosure of the information to the person making the request; or

(b) it is reasonable in all the circumstances to do so without the consent of the other individual.

# Background information

The Data Protection (Jersey) Law 2018 defines 'data' as meaning any information that:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a filing system or with the intention that it should form part of a filing system;
- is recorded information held by a scheduled public authority and does not fall into any of the above three categories.

# Personal data

The Jersey Law applies to 'personal data' meaning any information relating to an identifiable, natural, living person who can be directly or indirectly identified in particular by reference to an identifier (the 'data subject').

Images (stills/moving and with or without sound) from CCTV would fall into this definition.

**Jersey Office of the Information Commissioner**, 2nd Floor, 5 Castle Street, St Helier, Jersey JE2 3BT
**Telephone number:** +44 (0) 1534 716530 | **Email:** enquiries@jerseyoic.org