GRA
GIBRALTAR REGULATORY AUTHORITY

(14) GUIDANCE ON THE USE OF CCTV

Guidance on the EU General Data Protection Regulation 2016/679 & Data Protection Act 2004

10th November 2020
IR02/19 v2

CONTENTS

SUMMARY

- As with all personal data that is processed, the recording of identifiable images of individuals must have a legal basis. Once a data controller has identified a purpose, or purposes, for installing CCTV, the data controller must also identify and rely on an appropriate lawful basis for the processing of personal data that will take place. The EU General Data Protection Regulation 2016/679 ("GDPR") and the Data Protection Act 2004 ("DPA") list the lawful bases that organisations can rely on.
- CCTV should only be used when there is a clear and justified purpose. It is unreasonable and unjustified to install CCTV on a 'just-in-case' basis given that data controllers and data subjects must understand why the collection and processing of personal data is necessary.
- A data controller must limit the CCTV footage being recorded to only that which is necessary to achieve the specified purpose. Consideration should be given to the field of view of the cameras. For example, if you have CCTV cameras outside your shop to protect your premises, it may be necessary to limit the field of view of the cameras to only your shop entrance, and not unnecessarily capture more of the public street around the shop than is necessary. The recording of audio using CCTV should generally be restricted. Recording of conversations between individuals poses a high risk to the invasion of privacy.
- Personal data should only be held for as long as is necessary to achieve the identified purpose for which it is processed. Footage cannot be retained on a 'just-in-case' basis. A retention period should therefore be established. When the CCTV captures footage of a specific incident, it may be retained beyond the retention period if it is required for use in criminal or other proceedings but must be disposed of once it is no longer required.
- When CCTV is used, individuals must be informed about - the identity and contact details of the data controller, unless this is self-evident; the contact details of the Data Protection Officer, if relevant; the purposes and lawful basis for the use of CCTV; and, any other necessary information to do with the specific processing of the information. Generally, the most effective way of doing this is by using **prominently placed signs** at the entrance to the CCTV's zone.
- Data controllers are required to implement appropriate security measures to ensure that personal data are kept safe from any unlawful or unauthorised processing, accidental loss, destruction or damage. Ideally, recorded CCTV footage should only be accessible under strict controls.
- Data controllers also need to ensure that they can demonstrate that they are complying with the GDPR. A CCTV Data Protection Policy that outlines how the CCTV system is complying with data protection laws should be in place.
- Data controllers and data processors need to ensure that they have a **written contract** between them that complies with Article 28(3)(a) of the GDPR.
- In many cases, data controllers should perform a Data Protection Impact Assessment before installing any CCTV cameras.
- If a CCTV is recording images **strictly within** an individual's property, then the Domestic Exemption is likely to apply. However, if a CCTV recording captures images of an area beyond private property, such as a neighbouring parking space, garden, walkway or adjacent communal area, the Domestic Exemption is unlikely to apply.
- **Annex A** provides a step-by-step guide of what to consider when setting up CCTV.

1. INTRODUCTION

The Gibraltar Regulatory Authority, as the Information Commissioner (the "Commissioner")[1], issued a guidance document in relation to CCTV in 2007. However, the expanded use and capability of CCTV systems since then has society-wide implications, and unless such systems are used with proper care and consideration, they can give rise to concerns that an individual's privacy is being unreasonably eroded. The Commissioner's guidance has therefore been reviewed and updated accordingly.

This document provides good practice guidance for those involved in operating CCTV and other surveillance camera devices, to better understand their responsibilities and obligations in regard to data protection when using CCTV.

CCTV is used by many, ranging from household setups, to workplace and business security and monitoring systems, to large-scale public sector implementations, such as in city centres and travel control. The cost of basic CCTV cameras, including those with the ability to transmit captured data wirelessly, and to store and display it via internet services, is now well within the reach of ordinary members of the public. Further, although CCTV usage is generally considered to be advantageous in the reduction and prevention of crime, there are concerns about its intrusion into the privacy of individuals, particularly when it is used without appropriate controls or where unnecessary.

Data protection law, namely the Data Protection Act 2004 (the "DPA") which complements the Europe wide General Data Protection Regulation 2016/679 (the "GDPR"), provides a means of regulatory control over the use of CCTV systems so that individuals may enjoy security and safety without privacy and data protection rights being compromised.

Where video recording equipment is used, users should be aware of the potential application of data protection law to that recording. Any person or organisation using recording equipment, like CCTV, should remember that data may be considered 'personal data[2]' where some individual can be identified from it, and that simply recording and/or storing video and audio data may be considered 'processing[3]', even if no further use is made of that data. Therefore, both the context and quality of the recording can be highly relevant.

Before setting up a CCTV system in any given area, it is important that data controllers understand the information contained within this guidance note.

Acknowledgements

Where appropriate, Gibraltar's Information Commissioner will seek to ensure that locally published guidance notes are consistent with others made available by fellow Data Protection Commissioners in other jurisdictions.

As well as reflecting the existing data protection standards and practices in Gibraltar, parts of this document reflect and/or incorporate the guidance from the Irish Data Protection Commissioner's office "Guidance on the Use of CCTV - For Data Controllers".

[1] The Information Commissioner is the Chief Executive Officer of the Gibraltar Regulatory Authority.

[2] Article 4(1) of the GDPR.

[3] Article 4(2) of the GDPR.

2. COMPLYING WITH THE PRINCIPLES

Article 5 of the GDPR outlines seven key principles which lie at the heart of the data protection regime and must be duly considered by data controllers when processing personal data. These rules apply to the processing of personal data through the use of CCTV, and therefore operators of CCTV systems large and small, have clear and specific obligations to individuals whose data they record, store and/or transmit.

2.1 LAWFULNESS, FAIRNESS AND TRANSPARENCY OF PROCESSING

Lawfulness

As with all personal data that is processed, the recording of identifiable images of individuals must have a legal basis. Once a data controller has identified a purpose, or purposes, for installing CCTV, the data controller must also identify and rely on an appropriate lawful basis for the processing of personal data that will take place. The GDPR and the DPA list the lawful bases that organisations can rely on[4].

For instance, public authorities may have a lawful basis for the use of CCTV in order to carry out a task in the public interest, or in the exercise of official authority[5]. This will be subject to an assessment carried out by the public authority justifying the measure, taking into account any legal implications underpinning the function and the use of CCTV. The public authority's Data Protection Officer should be consulted when carrying out any such assessments regarding the implementation and use of CCTV.

Further, law enforcement agencies may have a lawful basis to use CCTV for the prevention, investigation, detection or prosecution of criminal offences under Part 3 of the DPA[6], which implements the Law Enforcement Directive (EU) 2016/680 ("LED").

In many cases, CCTV processing may be carried out by the owners and occupiers of premises in pursuit of their legitimate interests to support the protection of their property and goods against for example burglary, theft or vandalism, and to maintain the safety of persons using such property. Legitimate interests may provide a lawful basis for the processing of personal data, so long as the interests of the data controller (or third party) are balanced and not overridden by those of the data subjects.[7] When a data controller relies on legitimate interests as a lawful basis to implement CCTV, the data controller must ensure that (i) it is genuinely in their interest to do so, (ii) that it is necessary to achieve their identified purpose(s), and (iii) that it does not negatively impact the data subjects whose personal data is being processed. The legitimate interest(s), as well as the necessity of the CCTV processing, should be reassessed at periodic intervals.

[4] See the GRA Guidance Note IR01/18 on the General Data Protection Regulation (6) Identifying the Lawful Basis (https://www.gra.gi/gdpr-6-identifying-the-lawful-basis).

[5] Article 6(1)(e) of the GDPR.

[6] Section 44 of the DPA.

[7] Article 6(1)(f) of the GDPR.

Further, the fact that video imagery may involve the processing of special categories of personal data, including the revealing of racial or ethnic origin, or biometric data for the purpose of uniquely identifying a natural person, may mean that where CCTV is deployed on the basis of data subject consent as a lawful basis, data controllers will need to show that consent is both explicit and 'freely given, specific, informed and unambiguous'[8].

Fairness

Personal data processed by the use of CCTV must also be fair, meaning that the personal data is handled in ways individuals would reasonably expect and not used in ways that have unjustified adverse effects on them. Assessing whether you are processing information fairly depends partly on how you obtain it. In particular, if anyone is deceived or misled when the personal data is obtained, then this is unlikely to be fair.

Transparency

Transparency is fundamentally linked to fairness. Transparent processing of personal data is about being clear, open and honest with individuals from the start about who the data controller is, as well as how and why you are processing personal data. As a result, the following information must be given to individuals at the point of obtaining their images:

- The identity and contact details of the data controller, unless this is self-evident;
- The contacts details of the Data protection officer, if relevant[9];
- The identity of any local representative nominated by the data controller;
- The purposes and lawful basis for the use of CCTV;
- Any other necessary information to do with the specific processing of the information.

Generally, the most effective way of doing this is by using **prominently placed signs** at the entrance to the CCTV system's zone. **Cleary visible and readable signs** are particularly important where CCTV systems are very discreet, or in locations where people might not expect to be under surveillance.

Whilst it is up to the data controller to determine the most appropriate way to provide the information, an organisation may consider using a CCTV sign that only includes some of the relevant information (such as the identity and contact details of the data controller and purpose of the CCTV), but includes a website address where more detailed information is provided in a CCTV Privacy Notice (the "Notice"). Should this approach be taken, the Notice should also be available non-digitally in an easily accessible area, such as an information desk. Such information should be located where individuals can access it before entering the area being captured by the CCTV. Note Articles 12, 13 and 14 of the GDPR should be used as a basis for the creation of a compliant Notice, placing emphasis on making the Notice easy to understand and accessible to all whose personal data will be processed by the CCTV.

[8] See the GRA Guidance Note IR01/19 on the General Data Protection Regulation (13) Guidance on Consent (https://www.gra.gi/gdpr-13-guidance-on-consent).

[9] Article 37(1) of the GDPR introduces a requirement for organisations to appoint a data protection officer ("DPO") in certain circumstances. For further assistance, see Guidance Note IR03/17 "GDPR Guidance (3) Data Protection Officer" (https://www.gra.gi/dataprotection/guidance-on-the-general-data-protection-regulation/gdpr3).

2.2 PURPOSE LIMITATION

The principle of purpose limitation requires that personal data shall be "*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,"*[10] that is to say that personal data should only be collected when there is a clear and justified purpose. It is unreasonable and unjustified to install CCTV on a 'just-in-case' basis given that data controllers and data subjects must understand why the collection and processing of personal data is necessary. The clarity of purpose may also assist in overcoming any concerns raised by the data subjects about the processing of their personal data.

The purposes for installing and utilising CCTV can be varied, but more commonly include –

- aiding in the prevention of crime or theft; and
- supporting the maintenance of health and safety standards in the workplace.

More often than not, there will be more than one reason for the use of a CCTV system, but it is key that these be identified at the outset.

2.3 DATA MINIMISATION

The processing of personal data must be *"adequate, relevant and limited to what is necessary"*[11]*.* This means that a data controller must be able to justify that the use of CCTV is necessary to achieve the specified purpose and proportionate in its impact on the data subjects being recorded.

When assessing the need for a CCTV system, the principle of data minimisation should therefore be considered, requiring that data controllers limit the amount of personal data they process to achieve a purpose and that, if possible, the processing of personal data be avoided. If other measures such as supervision or the deployment of security staff – which does not involve the processing of personal data – have proven ineffective, this may indicate that the installation of CCTV is a proportionate response. Whether such measures are reasonable alternatives to CCTV should be assessed on a case by case basis.

Further consideration should also be given to the field of view of the cameras of the CCTV system. For example, if you have CCTV cameras outside your shop to protect your premises, it may be necessary to limit the field of view of the cameras to only your shop entrance, and not unnecessarily capture more of the public street around the shop than is necessary. Data controllers should avoid unnecessarily capturing footage of accessible areas, particularly if they are typically used for recovery or leisure activities, as well as places where individuals are likely to stay and/or communicate.

Data controllers must also be aware of the intrusive nature of the use of CCTV. In the workplace for example, employers may wish to only switch on cameras outside of working hours in order to protect the establishment, when no employees are present. In addition to this, avoiding the placement of cameras where individuals will have a higher expectation of privacy, such as changing rooms or toilets, will reduce the intrusive impact of the CCTV. The

[10] Article 5(1)(b) of the GDPR.

[11] Article 5(1)(c) of the GDPR.

threshold to justify the use of CCTV in such locations is at the highest level and generally very difficult to meet.

Further, in compliance with the principle of minimisation, the recording of audio using CCTV should generally be restricted. Recording of conversations between individuals poses a high risk to the invasion of privacy.

2.4 ACCURACY

The GDPR requires that the processing of personal data is accurate and where necessary, kept up to date[12]. In relation to CCTV for example, CCTV recordings may be used as evidence during criminal proceedings or during disciplinary disputes with employees, therefore it is essential that the recorded images are clear and accurate.

If the system uses features such as time references and/or location references, then these too must be accurate. Data controllers must also ensure that the equipment is in good working order.

2.5 STORAGE LIMITATION

Personal data should only be held for as long as is necessary to achieve the identified purpose for which it is processed. Although the GDPR does not specify or define any time periods, it must be noted that information cannot be retained on a 'just-in-case' basis. Data controllers may wish to take into consideration any previous issues or situations where the necessity for access to CCTV footage to achieve a purpose may provide an indication on how long personal data should be retained.

A retention period should therefore be established. The retention period should be the shortest period necessary to achieve a specific goal for which the system was initially installed. The retention period should also allow the data controller ample time to review footage as appropriate to be deleted. In the event that the CCTV system has a default retention period, the data controller should review this and compare and assess this against what is a necessary retention period to avoid the retention of the information for longer than is necessary.

Furthermore, when the CCTV captures footage of a specific incident, such as a workplace accident, or where the footage will be used as evidence in criminal proceedings, the data controller may be justified in keeping the information for longer than their decided retention period. However, this footage should be isolated from the general recordings and kept securely for the specific purpose(s) that it is needed.

[12] Article 5(1)(d) of the GDPR.

2.6 INTEGRITY AND CONFIDENTIALITY (SECURITY OF PERSONAL DATA)

Data controllers need to ensure that the utmost care is given to the safe storage of personal data and that the necessary precautions are taken to ensure the security of the information collected[13].

Data controllers are required to implement appropriate technical and organisational measures to ensure that personal data are kept safe from any unlawful or unauthorised processing, accidental loss, destruction or damage. Password protection and the use of encryption can limit the access to CCTV footage stored. However, generic or shared passwords should be avoided in order to reduce the risk of inappropriate use of the system occurring and going undetected. **In order to maintain and safeguard against inappropriate usage, the use and regular review of an access log provides assurance that only authorised personnel have access to and may view the footage.**

Technological advances in CCTV allows footage to be accessed remotely, via a mobile device for example. Although such technology is helpful in providing security monitoring of an empty building at night or during the weekends, there is an added risk of unauthorised disclosure which may arise from such functionality and further potential concerns from a data protection perspective may arise. Whilst employers may be tempted to use such technologies as a substitute for ground supervision by the managerial staff, this type of monitoring or surveillance is not likely to be justified.

A set of robust policies and protocols must be adhered to in order to ensure that the technical and organisational security measures are effective. Access controls and all policies must be reviewed and tested on a regular basis, and security measures should be enhanced or upgraded where necessary. Those that handle CCTV within an organisation should have clear guidance and training to ensure that they handle CCTV in a manner that ensures compliance with the GDPR. Equally, data controllers have a responsibility to only use data processors who provide sufficient guarantees to implement appropriate technical and organisational measures that ensure processing meets the requirements of the GDPR.[14] Data processors must therefore also ensure that amongst other things, they also have robust measures in place to keep personal data safe. Please refer to section 6 below for further information.

The Commissioner has found that organisations are in some cases failing to implement appropriate security measures to protect against –

(a) unauthorised access to CCTV footage (e.g. staff snooping); and
(b) unauthorised disclosure/leaks of CCTV footage.

Organisations need to ensure that they have appropriate security measures in place to protect against the abovementioned risks. It is a matter for data controllers and processors to determine what arrangements are suitable to their circumstances, however the Commissioner recommends the following measures:

(a) Access controls:

[13] For further information, please see the GRA Guidance Note IR07/19 on the General Data Protection Regulation (18) Guidance on Data Security (https://www.gra.gi/data-protection/gdpr-dpa-18-data-security).

[14] Article 28(1) of the GDPR.

- Recorded footage should only be accessible to a limited number of staff through strict access controls.
- No single person shall have access to the recorded CCTV footage. A "two-man access control system" should be implemented[15]. For example:

    - One designated individual shall be in possession of the username and password used to log in to the only computer which operates the software required to access the CCTV footage recorded.
    - Another designated individual shall have the username and password required to log in to the aforementioned software.

    OR

    - One individual has access to the locked facility where the SD card storing the CCTV footage is kept (without which recorded footage cannot be accessed).
    - Another designated individual shall have the username and password required to log in to the software that is required to access and view the footage once the SD card is provided.

- Logs of access to CCTV footage data will be automatically generated by the computer system and shall be periodically reviewed and scrutinised to ensure that there is no unwarranted access to CCTV footage.
- A detailed manual log will be kept of every time CCTV footage is accessed, disclosed and/or otherwise used.

(b) Mobile devices:

- No mobile phones or other devices capable of recording images will be allowed in the area where CCTV footage may be viewed.

(c) Training:

- Individuals with access to recorded footage will receive appropriate data protection training to ensure that they are aware of the importance of data protection and privacy.
- Individuals with access to recorded footage will receive appropriate training on the security measures employed to protect the CCTV footage from unauthorised/unlawful use/access.

(d) Disciplinary policy:

- Disciplinary policy and procedure in place to address incidents where an individual does not comply with the established rules regarding access and use of CCTV footage.

2.7 ACCOUNTABILITY

The GDPR introduced new operational obligations upon data controllers to demonstrate that they have adopted and maintained technical and organisational measures, enabling them to

[15] This mitigates the risk of any one individual unlawfully processing CCTV footage as two individuals are required to access the CCTV footage.

meet their responsibilities under the GDPR. The principle of accountability in this regard, assumes a much greater prominence in the regulatory framework.

Larger data controllers need to ensure that a record of all their processing activities is maintained; any use of CCTV and accompanying data protection risks therefore need to be included in the record. If the data controller has carried out an assessment in relation to the installation of CCTV, this should be completed in a way that clearly sets out the need, proportionality, reasoning and the assessment criteria justifying the decision.

3. CCTV DATA PROTECTION POLICY

Best practice dictates that a data controller shall set out their position on the issues surrounding the use of CCTV in the form of a CCTV Data Protection Policy (the "Policy"). The introduction of suitable policies can be a key precaution when the processing of data takes place,[16] and will assist in demonstrating compliance with the GDPR, in line with the accountability principle. A Policy should identify the reasons why a CCTV system has been implemented, how the CCTV footage is processed and how the system will be managed. Further, the scale of the CCTV system and its impact on individuals whose images may be captured will help determine the level of detail that should be included in the Policy.

A Policy that relates to a place of work should be brought to the attention of all employees so that they are fully informed about the processing of personal data by this means and are aware of their responsibilities. The Policy may also be published on an official company website to appropriately advise members of the public who may attend the premises, informing them about how the CCTV system is used. This will also assist the Commissioner in understanding how the data controller has applied the principles relating to processing of personal data to the use of CCTV in the event of an investigation or inspection.

A Policy (and all other data protection policy documents implemented) should be reviewed from time to time, to guarantee that the policies are being applied as they are intended to be and evolve in light of any changes in law or legislation. In addition to this, the reason for the initial implementation of CCTV may change over time, which means a reassessment of the necessity of the CCTV will need to be carried out and reflected in the Policy.

4. PRIVACY BY DESIGN & DEFAULT

The principle of privacy by design and default is underpinned by the GDPR. Data protection by design requires that appropriate measures to implement data protection principles are integrated at the planning stage of any data processing operation and maintained at all stages. This means that where the implementation of CCTV is being considered, data protection concerns are addressed at the earliest stage of the project. This pre-processing risk assessment designed to identify and minimise risks to privacy and data protection non-compliance can be satisfied by conducting a Data Protection Impact Assessment (see Section 5).

[16] Article 24(2) of the GDPR.

Data protection by default on the other hand, requires that technical and organisational measures be put in place to ensure that only personal data which are necessary for a specific purpose are processed. The data controller shall therefore review and ensure that the default settings of the CCTV or applications that process personal data are privacy friendly. In the rollout of a CCTV system, this will have a bearing, for example, on the placement of cameras, the focus of the cameras, the capability of the cameras, the functionality of the cameras and privacy masking features as well as the determination of an appropriate retention period. Users of CCTV should be aware that the use of particular features, such as zoom capability, can increase the potential intrusion on individuals' privacy.

5. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

If data collection or processing in any form is likely to result in a high risk to the rights and freedoms of individuals, such as CCTV systems conducting large-scale, systematic monitoring of public spaces, or when CCTV is capturing vulnerable data subjects, then a DPIA may need to be carried out before the system is installed. For further information, see previous guidance provided on DPIAs.[17]

The purpose of a DPIA is to identify and minimise the risks to the privacy infringement and violation of personal data protection and must be performed before personal data processing takes place. The DPIA should include an evaluation of:

- scheduled processing and purpose of processing;
- the necessity of personal data processing and principle of fairness;
- risks to rights and freedom of data subjects;
- safeguards to mitigate such risks.

The DPIA should also include the opinion of the affected data subjects or their representatives. For CCTV systems for example, it applies to employees or the general public, who are the subjects of monitoring.

6. DATA PROCESSORS

A data controller is any individual or organisation that determines the purposes and means of the processing of the personal data and will have primary responsibility for compliance with data protection laws. However, often a CCTV system is managed and maintained by a third party on behalf of the data controller (for example, a security company may manage and maintain a CCTV system on behalf of the management company of an estate.) Organisations

[17] See the GRA Guidance Note IR04/17 on the General Data Protection Regulation (4) Data Protection Impact Assessment (https://www.gra.gi/dataprotection/guidance-on-the-general-data-protection-regulation/gdpr4), as well as the accompanying documents located on that webpage.

that install and operate CCTV systems, on behalf of others, are considered data "processor[s][18]". Data processors process personal data on behalf of the data controllers, subject to contract.

The GDPR reinforces the responsibilities of data controllers with regard to data processors and specifies particular information that must be contained in **a contract between them**. The contract should outline what the data processors can do with the data that is collected through the use of CCTV, what security standards should be put in place, and how long the data should be retained for. **Please refer to Article 28(3) of the GDPR** for all terms that such contracts should contain. It is therefore **essential** to understand who the data controllers and data processors are in relation to the running and management of CCTV.

The ability of data processors to sub-contract will be subject to prior written consent from the data controller, and a data processor is required to inform the controller of any new sub-processors, giving the controller time to object. Where a data processor subcontracts work, their sub-processor contracts must contain the same contractual obligations they have with the controller and remain liable to the controller for the actions or inactions of their sub-processor. This has direct implications for organisations that sub-contract their CCTV provision, and for CCTV service companies that sub-contract aspects of their service. It will also have implications for organisations that use data processors for cloud-based processing of their CCTV footage.

7. DISCLOSURE TO THIRD PARTIES

Disclosure of CCTV recordings to third parties should always be consistent with the purposes for which the CCTV system was set up[19]. It is unlikely the releasing of images on social media would comply with data protection laws.

In certain circumstances however, a data controller may be required to provide CCTV recordings to third parties for a purpose other than that for which they were originally obtained. For instance, a law enforcement agency may request CCTV footage in order to assist the investigation of a criminal offence. Under these circumstances, the data controller should verify the request and it is recommended that requests for copies of CCTV footage should only be acceded to where a formal written request is provided to the data controller stating that the CCTV footage is needed by the law enforcement agency for the investigation of a criminal matter. In an event that there is an urgent request for the footage, then a verbal request may suffice. However, it is important that any verbal requests are followed up with a formal written request. In any event, data controllers may refuse to provide the images, and request that the law enforcement authority provide a court order or warrant. Responding to such court orders/warrants would not breach the GDPR.

In accordance with the principle of accountability, such requests should be documented and maintained by data controllers and processors detailing any provision of footage.

[18] Article 4(8) of the GDPR.

[19] If the data controller is considering whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, the data controller must take into account the requirements at Article 6(4) of the GDPR.

A data controller may be asked to provide CCTV footage to a third party, not classified as a law enforcement agency, in order to investigate an incident. Under these circumstances, the same assessment procedure applies whereby the pursuit of a legitimate interest of the data controller or third party can be justified. These events need to be assessed on a case-by-case basis to guarantee that the principles of data protection are followed and that the rights of data subjects are not prejudiced. It should be noted that the legitimate interests of a third party do not oblige a data controller to disclose CCTV footage but may permit such disclosure subject to assessment.

In all circumstances involving the disclosure of CCTV footage, the method of disclosing images should be secure so as to ensure the security of the footage being disclosed and ensure that only the intended recipient is able to access the footage. It is recommended that logs of requests for and disclosure of images, are kept in line with the accountability principle.

8. RIGHT OF ACCESS/DATA SUBJECT RIGHTS

Data subjects have a right of access to their personal data. This applies to any person whose identifiable image has been recorded by a CCTV system. When a subject access request ("SAR") is received[20], the data controller must respond to the request without undue delay and in any event, within one month, and may refuse the SAR in certain circumstances[21]. Enough information should be provided by the data subject to ensure data controllers can identify the data subject as the subject of the images and also to locate the images on the CCTV system.

To facilitate the processing of the SAR, the data controller may ask the data subject to give a reasonable indication of the data and time of the footage they are after. If the retention period has expired, and the footage has been deleted, the individual should be informed that the footage no longer exists. However, if a request has been received, the footage in question should not be deleted until the SAR has been satisfied.

Responding to a SAR involves providing a copy of the footage in video format and detailed information on the lawful basis and purpose for the filming, as well as any disclosures that have been made to third parties. Where it is not possible to provide the footage in video format, it may be acceptable to provide still pictures as an alternative. In the event that still pictures are provided, the data controller will need to supply sufficient stills for the duration of the recording in which the data subject's image appears in order to comply with the SAR.

If the data requested by the data subject also includes other individuals, the data controller should pixelate, blank out or otherwise de-identify, where necessary, the images of other individuals before providing a copy of the footage to the data subject. Alternatively, the data controller may also seek consent of those who appear in the CCTV footage to release an unedited copy containing their images to the data subject.

[20] Requests under Article 15 of the EU General Data Protection Regulation 2916/679 are commonly referred to as "Subject Access Requests".

[21] Article 12(3) and (4) of the GDPR.

Data controllers of CCTV systems should have a procedure in place in order to ensure that all SARs are responded to without undue delay. The data controller may seek assistance from a third-party processor to edit the footage and retrieve or review the data subject's images.

Information regarding SARs may also be provided through a public website to facilitate members of the public in making access requests.

Data subjects also have a right to have images erased in certain circumstances, within one month and without undue delay[22]. Whilst this only applies in certain circumstances, data controllers should have measures in place to facilitate such requests, should they arise.

9. CCTV & THE DOMESTIC EXEMPTION

As mentioned earlier, any person or organisation using recording equipment like CCTV, should remember that images or recordings may be considered 'personal data' and simply recording and/or storing images and audio data may be considered 'processing' under the GDPR and the DPA. Therefore, the various rights and duties under data protection law apply.

One thing which should be kept in mind however, is whether or not the images fall under the 'personal' or 'household exemption' of the GDPR (the "Domestic Exemption").[23] This exemption states that the GDPR does not apply to processing of data (including the processing of personal data through CCTV systems) "*in the course of a purely personal or household activity*". If the recording **does not fall** within this category, then it is likely that the person making the recording has obligations as a 'data controller' under the GDPR.

When assessing whether or not recording is **purely** of a personal or household nature, a number of factors should be taken into consideration, such as:

- whether the recording has any connection to a professional or commercial activity;
- whether the people involved in or captured by the recording were known to the person making the recording; and
- what area the recording covered – did it cover public areas, a private space or both?

If a CCTV is recording images **strictly within** an individuals property, then the Domestic Exemption is likely to apply. However, if a CCTV recording captures images of an area beyond private property, such as a neighbouring parking space, garden, walkway or adjacent communal area, the Domestic Exemption is unlikely to apply. Even if the Domestic Exemption applies, it is strongly recommended that the requirements of data protection law are considered as a matter of good practice.

[22] Article 17 of the GDPR.

[23] Article 2(2)(c) and Recital 18 of the GDPR.

10. COVERT SURVEILLANCE

Using CCTV to record individuals without their knowledge is generally unlawful and in breach of data protection laws. However, in exceptional circumstances, covert surveillance may be permitted where the data is processed for the purposes of preventing, detecting or investigating offences and apprehending or prosecuting offenders. Should one of these exceptional circumstances apply, a written internal policy should be implemented. This should detail the purpose of the CCTV, the justification for its use, the procedure used and the measures and safeguards that will be implemented, together with the specification that the final objective of the surveillance is a law enforcement agency acting on the data collected for potential criminal investigations or civil legal proceedings arising as a consequence of an alleged committal of a criminal offence.

The decision on whether to undertake covert surveillance should be made on a case-by-case basis. A DPIA should be carried out before its installation, to clearly assess whether its implementation can be justified as necessary and proportionate to achieve the intended purpose. Covert surveillance must be focused and of short duration and therefore only relevant and specific individuals or locations should be recorded and if no evidence is recorded within a reasonable timeframe, the covert surveillance should cease. If the surveillance is intended to deter crime, overt cameras may be a more appropriate and less invasive measure.

It must be noted that if a data processor is involved in covert surveillance, the data controller must remember that a data processor contract will also be required.

11. FACIAL RECOGNITION AND BIOMETRIC DATA

Specific technical features of certain CCTV systems, such as the use of facial recognition software, may impact the basis on which the data can be lawfully processed. Processing facial recognition requires a matching step where previously seen faces are registered and recorded on the system so that if an individual was to appear on more than one occasion, the CCTV system would recognise and uniquely identify the individual in question.

Facial recognition processing is considered biometric processing and therefore, the data processed is categorised as "special category" of personal data. It is therefore subject to the requirements of the GDPR, which prohibits its use unless it is for a specific condition for the lawful processing of the data, set out in the GDPR.[24]

Any processing of biometric data should be considered as unique to the overall usage of the CCTV system and a data controller dealing with such data must take all steps to ensure that it is GDPR-compliant. Processing personal data of this nature is likely to be high-risk and therefore, a DPIA will likely be required. Please refer to section 5 above.

[24] See the GRA Guidance Note IR01/18 on the General Data Protection Regulation (6) Identifying the Lawful Basis (https://www.gra.gi/gdpr-6-identifying-the-lawful-basis).

12. DASHBOARD CAMERAS, ACTION CAMERAS AND DRONES

DASHBOARD CAMERAS

A dashboard mounted camera commonly known as a "dash cam", is an inexpensive way to combat vehicle accident insurance fraud or mitigate personal security concerns. If you are recording with a dash cam, you are likely to be a data controller for the purposes of data protection legislation and should therefore give due consideration to the legal responsibilities that you may be taking on. Data controllers are required to be compliant with data protection legislation and process personal data in accordance with the principles of data protection outlined above.

Users of dash cams must therefore consider the following:

- Personal data must be processed in a transparent manner. In the first instance, there should be a clearly visible sign or sticker on and/or inside the vehicle, as applicable, to indicate that filming is taking place.

- A policy sheet detailing your contact details, the basis on which you are collecting the images and audio of others (if relevant), the purposes for which the data is being used and how long you will retain it for, should be prepared by you and made available on request to anyone who asks for further information[25]. Alternatively, you may provide the information verbally.

- In the event of an accident, you should advise the other party that you have recorded footage of the accident.

- Personal data should only be retained for as long as required and for the purpose that it was obtained. You will need to think about how long you keep hold of footage. Footage of an accident may be required for a claim or investigation and can be retained for that purpose. Other footage should not be retained indefinitely and should be routinely deleted.

- Personal data must be kept securely. Be aware of, and limit, who has access to your camera and any external storage devices.

- You may have to provide a copy of footage/images to anyone who requests their personal data, within one month in response to a SAR. You should also avoid sharing the data of other people, which may need to be redacted from the footage.

- If you are using a dash cam for security or accident liability purposes, you should be aware that the publication of footage, for example on social media platforms, represents a further processing step, and risks infringing the privacy rights of recorded individuals and data protection legislation.

[25] Articles 12 and 13 of the GDPR.

ACTION CAMERAS AND DRONES

Although there are no specific guidelines on the use of 'action cameras' (such as GoPros) or drones capable of recording video, many of the considerations relevant to CCTV and dash cams apply equally to the use of these types of video recording equipment.

Nonetheless, the Commissioner recommends that action cameras and drones in particular, are operated in a responsible way to respect the privacy of others. Users should take the following into account -

- **Let people know before you start recording**. Under some circumstances this will be fairly easy because you may know everyone within the field of view of the drone camera. However, in other scenarios, for example at a beach, this is much more difficult so a commonsense approach must be taken.

- **Consider your surroundings**. If you are planning on recording images beyond your property, a drone may intrude on the privacy of others where they expect their privacy to be respected.

- **Get to know your camera first**. It is a good idea to understand the capabilities of your camera in a controlled situation to understand how it works. Ask yourself –

    - *What is the quality of the images recorded?*
    - *How powerful is the zoom?*
    - *Can you control when it starts and stops recording?*

    Drone cameras are capable of taking extraordinary pictures from vantage points. Knowing the capabilities of your camera will help to limit the risk of privacy intrusion.

- **Plan your flight**. A drone's battery life is likely to be short. By understanding the capabilities of its flight time, it will be easier to plan how to avoid invading the privacy of other individuals.

- **Keep you and your drone in view**. If you and your drone are visible it will be easier for members of the public to be aware that they may be the subject of a drone recording and be able to identify you as the person who is piloting the drone.

- **Think before sharing**. Once your drone has landed, think carefully about who's going to be looking at the images, particularly if you're thinking about posting them on social media. Avoid sharing images that could have unfair or harmful consequences. Apply the same common-sense approach that you would with images or video recorded by a smartphone or camera.

- **Keep the images safe**. The images you have taken may be saved on an SD card or USB drive attached to the drone or the camera. If they are not necessary, then don't keep them. If you do want to keep them, then make sure they are kept in a safe place.

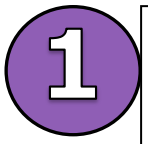
Further information on the use of drones in Gibraltar can be found here. In addition to this, assistance on drone usage and compliance with the GDPR can also be found here.

IMPORTANT NOTE

This document is purely for guidance. The document does not constitute legal advice or legal analysis. All organisations that process personal data need to be aware that the GDPR and the DPA will apply directly to them. The responsibility to become familiar with the GDPR and the DPA and comply with its provisions lies with the organisation.

Where necessary, the Commissioner will review this Guidance Note in accordance with any updates or other developments. In the event of any conflict or inconsistencies between this Guidance Note and the GDPR and the DPA, the GDPR and the DPA will take precedence.

ANNEX A – CCTV: WHAT TO CONSIDER?



LAWFULNESS, FAIRNESS & TRANSPARENCY

Can you provide a lawful basis for your use of a CCTV system?

Is the lawful basis you're relying on the most appropriate one?

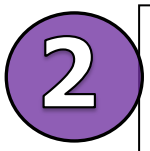
How will you inform individuals that you are recording their images?

Have you considered how an individual might be able to contact you for more information, or to request a copy of the CCTV footage?

Are you complying with the GDPR's transparency obligations?

Is anyone being deceived or misled by the use of CCTV?

Do you have CCTV signs at your establishment? If so, are they clearly visible and readable?



PURPOSE LIMITATION

Can you give a clear reason why the use of CCTV is required?

What will the CCTV system be observing?

Have you identified a purpose, and provided justification, for the use of CCTV?

Will the CCTV system be used for security purposes only?

Will the use of the personal data collected by the CCTV be limited to the initial purpose identified?

DATA MINIMISATION

Is the processing of personal data by CCTV adequate, relevant and limited to what is necessary in relation to the purpose(s)?

If your CCTV system is to be used for purposes other than security, are you able to justify that those other uses are adequate? For example, using CCTV to monitor staff in the workplace is considered to be highly intrusive. The use of CCTV for health and safety reasons would warrant evidence that the installation of a CCTV system is proportionate.

Will the recording of CCTV footage be measured and reasonable in its impact on the people recorded?

Are there any other ways you can achieve your goal without the use of CCTV?

Can you demonstrate that CCTV is necessary to achieve your goal?

ACCURACY

Are reasonable steps being taken to ensure that the personal data is accurate and kept up to date?

Are the timestamps or location references on the recordings accurate?

5 STORAGE LIMITATION

How long will the CCTV system recordings be retained for?

Are you aware that retaining personal data on a "just-in-case" basis is not deemed good practice?

Did you know the retention period should be the shortest period necessary to achieve a specific goal?

6 INTEGRITY & CONFIDENTIALITY

What appropriate technical and organisational measures will you be putting in place to ensure that the data collected via the CCTV system is stored in a safe and secure manner?

Who will have access to the CCTV recordings?

How will the CCTV footage be recorded, stored and managed?

7 ACCOUNTABILITY

Are you able to demonstrate that you have adopted and maintained appropriate technical and organisational security measures for the use of CCTV?

Do you hold a record of processing activities?

CONTACT US

Gibraltar Regulatory Authority
2nd floor, Eurotowers 4, 1 Europort Road, Gibraltar

(+350) 20074636
privacy@gra.gi
www.gra.gi