Code of Practice issued by the Data Protection Commissioner for CCTV Systems operated by the Mauritius Police Force

Table of Contents

Page

Index

Foreword

The growing use of CCTV systems has wide societal implications. Unless such systems are used with due care and consideration, they may give rise to concern of the individual's "private space" being unreasonably eroded or interfered with.

Recognisable images captured by CCTV systems are "personal data" relating to an identified or identifiable individual who is a "data subject" and CCTV systems' operators are "data controllers", who is, in this case, the Police Force. The use of CCTV systems is therefore covered by the provisions of the Data Protection Act but subject to certain exceptions provided in section 46 of the Act.

The purposes for recording personal information through CCTV must be strictly confined to the prevention or detection of crime; or the apprehension or prosecution of offenders; and/or national security. Other purposes will be illegitimate and in contravention of the provisions of the Data Protection Act. It is the responsibility of the Commissioner of Police to monitor the compliance of this Code of Practice and to register with the Data Protection Commissioner as a data controller.

Mrs. Drudeisha Madhub
Data Protection Commissioner

INTRODUCTION

This Code of Practice sets out the basic conditions for the use of CCTV systems operated by the Police. All persons involved in the planning, supervision or operation of such a CCTV scheme should familiarise themselves with this document from the outset. It is of crucial importance in order to maintain public confidence in the operation of CCTV systems that there is no improper use of the equipment. Any misuse of CCTV systems is likely to damage the positive perception of CCTV in the eyes of the public. Compliance with this Code of Practice governing CCTV systems and their operation will not only assist the Police to act in accordance with law but will also help in maintaining trust of the public in these systems.

Purpose of the Code of Practice

This Code of Practice has been designed to assist police operators of CCTV systems by highlighting certain legal obligations set down in the Data Protection Act. In order for this Code to remain relevant to the day to day activities of CCTV operation, it may require constant update. Accordingly, this Code will be kept under review to ensure that it remains relevant in the context of changes in technology, and compliant with any developments in this area. Contravention of a provision of the Data Protection Act may expose a person to prosecution under the Act.

Use of the CCTV System

The Data Protection Act provides in its section 46 that:-

The processing of personal data for the purposes of –

(a) the prevention or detection of crime; or

(b) the apprehension or prosecution of offenders; shall be **exempt from** :-

  (i) the Second, Third, Fourth and Eighth data protection principles found in the First Schedule;

  (ii) sections 23 to 26; and

  (iii) Part VI of this Act in respect of blocking personal data, **to the extent to which the application of such provisions would be likely to prejudice any of the matters specified in paragraphs (a) to (b).**

It is to be noted that the three exceptions elaborated above must be read subject to the proviso contained in the last paragraph.

Furthermore, as spelt out in section 56 (3) (b) of the Act, the Commissioner specifies that this code of practice shall come into operation on the **24th of April 2009**.

(1) Initiation of a CCTV System

- Only persons authorised by the Commissioner of Police shall be permitted access to the control area where monitoring takes place.
- Police will at all times ensure the proper and responsible operation of the CCTV system under his control and ensure that all persons operating or monitoring the system are appropriately trained in the system's use and understand the restrictions and legal obligations imposed upon them by law.
- It is the responsibility of the Police to ensure that all uses of the system are appropriate and in the interest of society.
- A designated person should be nominated by the Commissioner of Police. This individual will have responsibility for ensuring the proper, efficient and orderly day to day operation of the CCTV system.
- The Police officers responsible for the system shall maintain an appropriate record of the system's effectiveness.
- Respect for the individual's liberty and privacy where no criminal offence has been or is being committed should be a primary consideration.

(2) Siting Standards

- Cameras should be sited in such a way that they only monitor those spaces which are intended to be covered by the system.
- Operators must be aware of the purposes for which the scheme has been established. Operators must be aware that they may only use the cameras in order to achieve the purposes for which the system has been installed.
- Operators must also be aware of the position a camera is left in after use. A camera when not in use should be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.
- Clear and prominent signs should be placed so that the public are aware that they are entering an area which is covered by a CCTV system. These signs should be clearly visible and legible to members of the public. Such signs should contain the following information:
  - ➢ the identity of the organisation responsible for the CCTV scheme, i.e, the Commissioner of Police;
  - ➢ the purposes of the scheme;
  - ➢ details of who to contact regarding the scheme.

(3) Quality of the Images

- Upon installation, an initial check should be undertaken to ensure that all equipment performs properly.
- If tapes/cds/dvds are used, it should be ensured that they are good quality tapes/cds/dvds.
- The medium on which the images are captured should be regularly cleaned so that images are not recorded on top of images recorded previously.
- The medium on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated.
- If the system records features such as the location of the camera and/or date and time reference, these should be accurate.
- If the system includes location and date/time reference features, users should ensure that they have a documented procedure for ensuring their accuracy.
- Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.
- When installing cameras, consideration must be given to the physical conditions in which the cameras are located.
- Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times.
- Cameras should be properly maintained and serviced to ensure that clear images are recorded.
- Cameras should be protected from vandalism in order to ensure that they remain in working order.
- A maintenance log should be kept by the Police Officers responsible for the system.
- If a camera is damaged, there should be clear procedures for:
  - ➢ defining the person responsible for making arrangements for ensuring that the camera is repaired;
  - ➢ ensuring that the camera is repaired within a specific time period;
  - ➢ monitoring the quality of the maintenance work.

(4) Processing of CCTV Images

- All tapes/cds/dvds will be stored in lock fast facilities to which access is restricted within the CCTV control area at all times except when:-
  - ➢ They are requested by an officer of Police not below the rank of Assistant Commissioner of Police and such a request being authorised by a police officer of at least the rank of Inspector;
  - ➢ They are requested through the judicial process.
- Tapes/cds/dvds held should be counted daily and a record kept by Police Officers responsible for the system or designated person.
- Images should not be retained by the Commissioner of Police for longer than is necessary. Images will be erased and tapes re-used after such a reasonable period of days as may be determined by the Commissioner of Police unless required for the investigation of offences or evidential purposes.
- Access to the recorded images and the tapes/cds/dvds should be restricted by the Commissioner of Police to a designated person or persons. Other persons should not be allowed to have access to that area when a viewing is taking place.
- Copies of tapes/cds/dvds are not to be made by the Police. If copies are to be made, the Police Officer responsible for the system will do so in any of the following circumstances:
  - ➢ the incident recorded is of a serious nature (eg. one that may lead to criminal proceedings);
  - ➢ a formal request from the Police (of at least the rank of Assistant Commissioner of Police);
  - ➢ recording is proceeding to trial;
  - ➢ a request to view the tape is received from the DPP;
  - ➢ the circumstances are such that repeated playing of the incident recorded on tape/cd/dvd is required (i.e. to show to witnesses);
  - ➢ where a copy is required in order to satisfy a request for access to personal data which is also subject to a prescribed fee.
- An original tape/CD/DVD shall remain in the possession of the Police or a person designated to act on its behalf unless the original is required:
  - ➢ for the purpose of court proceedings;
  - ➢ by or under any other enactment.

- On removing the medium on which the images have been recorded, the police officer responsible for the system must ensure that they have documented:
  - ➢ the date on which the images were removed from the general system;
  - ➢ the reason why they were removed from the system;
  - ➢ any crime incident number to which the images may be relevant;
  - ➢ the location of the images;
  - ➢ the signature of the collecting official, where appropriate.

  Removal of the medium on which images are recorded, for viewing purposes, should be documented as follows:
  - ➢ the date and time of the removal.
  - ➢ the name of the person removing the images.
  - ➢ the name(s) of the person(s) viewing the images. (If this includes third parties, the name of the organisation to which the third party belongs).
  - ➢ the reason for the viewing.
  - ➢ the outcome, if any, of the viewing.
  - ➢ the date and time the images were returned to the system or secure place, if they have been retained for evidential purposes.
- All operators and employees with access to images should be made aware by the Police of the procedures which need to be followed when accessing the recorded images.
- It is the responsibility of the Commissioner of Police to ensure that all operators are made aware of :
  - ➢ the user's security policy (eg. procedures for access to recorded images).
  - ➢ the user's disclosure policy.

(5) Disclosure of Images to Third Parties

- Disclosure of the recorded images to third parties should only be made by the Police in limited and prescribed circumstances. Circumstances in which disclosure is appropriate would be a requirement under any enactment or court order to disclose the images with regard to:
  - ➢ a formal request from a member of the Commissioner of Police (of at least the rank of Assistant Commissioner of Police), for disclosure of images, on the grounds that the images are likely to be of use for;
    - the investigation of a particular offence;
    - the purpose of obtaining legal advice;
    - the purpose of exercising or defending legal rights.
- if required by the Attorney-General's Office whenever a case/action is being taken against the Commissioner of Police;
- the media, where it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident should be taken into account. The release of images to the media in a criminal investigation is solely within the remit of the Commissioner of Police;
- Where the images are determined to be personal data and it is decided that images will be disclosed to the media, the images of individuals apart from the victim, witness or perpetrator may need to be disguised or blurred so that they are not readily identifiable;
- people whose images have been recorded and retained (unless disclosure to the individual would prejudice criminal inquiries or criminal proceedings).
- All requests for disclosure should be recorded by the Commissioner of Police. If disclosure is denied, the reason should be documented.
- If disclosure of the images is allowed, then the following should be documented:
  - ➢ the date and time on which disclosure was made;
  - ➢ the identification of any third party to whom disclosure was made;
  - ➢ the reason for allowing disclosure;
  - ➢ the extent of the information which was disclosed;
  - ➢ the identity of the officer authorising such disclosure.

- If the system does not have the facilities to carry out that type of editing, an editing company as data processor may be hired to carry it out.

- Where an editing company is hired, then the Police needs to ensure that:

  ➢ there is a contractual relationship between himself and the editing company;

  ➢ that the editing company has given appropriate guarantees regarding the security measures they take in relation to the images;

  ➢ the Police shall have in place appropriate and adequate security and organisational procedures to ensure those guarantees are met including a right of access to the contractor's premises or systems;

  These include having appropriate security measures in place to prevent unauthorised access to, alteration of, disclosures of, accidental loss, and destruction of the data in his control. Security measures are appropriate to:-

  (i) counteract any harm that might result from such unauthorised access to, alteration of, disclosure of, accidental loss, and destruction of data;

  (ii) the nature of the data concerned.

  ➢ the written contract makes it explicit that the editing company can only use the images in accordance with the instructions of the Commissioner of Police or a designated police officer acting on his behalf;

  ➢ the written contract makes the security guarantees provided by the editing company explicit.

(6) Access by Data Subjects

- All police officers involved in operating the equipment must be able to recognise a request by data subjects for access to personal data in the form of recorded images.
- The Police must then inform the data subject:
  - ➢ whether the data kept by him include personal data relating to the data subject;
  - ➢ the purposes for which the data are processed;
  - ➢ the recipients to whom the data are disclosed.
- A request for such information may be refused where the Police is not supplied with the information that he may reasonably require in order to satisfy himself as to the identity of the person making the request and to locate the information which the data subject is seeking; or where compliance with such a request will be in contravention of a confidentiality obligation imposed under any other enactment.
- Data subjects must fill in a request for access to personal data form as provided in the Data Protection Regulations 2009.The Police must then:
  - ➢ locate the images requested;
  - ➢ indicate that a fee will be charged for carrying out the search for the images requested. The fee to be charged for the supply of copies of data in response to a subject access request is set out in the Data Protection Regulations 2009;
  - ➢ ask whether the individual would be satisfied with merely viewing the images recorded;
  - ➢ indicate that the response will be provided promptly following receipt of the required fee and within 28 days of receiving the request .
- Police officers operating the system should be able to explain to members of the public the type of images which are recorded and retained, the purposes for which those images are recorded and retained, and information about the disclosure policy in relation to those images.
- All data subject access requests should be dealt with by a designated police officer.
- The designated police officer should locate the images requested.

- The designated police officers should determine whether disclosure to the individual would entail disclosing images of third parties.
- If third party images are not to be disclosed, the designated police officer shall arrange for the third party images to be disguised or blurred.

(7) Miscellaneous Data Subjects' Rights

- All police officers involved in operating the CCTV equipment must be able to recognise a request from an individual to rectify, block, erase or destroy where appropriate, inaccurate personal data.
- All police staff must be aware of the identity of the designated police officer who is responsible for responding to such requests.
- In relation to a request for rectification, blockage, erasure or destruction, the designated police officer should indicate whether he or she will comply with the request or not.
- The designated police officer must provide a written response to the individual as soon as reasonably practicable setting out his decision on the request.
- If the designated police officer decides that the request will not be complied with, he must set out the reasons in his response to the individual.
- A copy of the request and response should be retained and filed securely.
- The designated police officer shall document:
  - ➢ the request from the individual;
  - ➢ the original decision;
  - ➢ his response to the request from the individual;
  - ➢ the reasons for rejection, if applicable.

(8) Monitoring Standards

- The contact point indicated on the sign should be available to members of the public during office hours. Police officers staffing that contact point should be aware of the policies and procedures governing the use of the CCTV equipment.
- The relevant fees to be charged in respect of the provision of any of the above documents are provided in the Data Protection Regulations 2009.
- A complaints procedure should be clearly documented by the Commissioner of Police who may seek the assistance of the Data Protection Commissioner on this matter.
- A record of the number and nature of complaints or enquiries received should be maintained by the Commissioner of Police together with an outline of each action taken.
- A report on those numbers should be collected by the designated police officer in order to assess public reaction to, and opinion of, the use of the system.
- A designated police officer should undertake regular reviews of the documented procedures to ensure that the provisions of this Code of Practice are being complied with. Such an audit should be carried out on at least an annual basis.
- A report on those reviews should be provided to the Police in order that compliance with legal obligations and provisions of this Code of Practice can be monitored.
- An internal annual assessment should be undertaken which evaluates the effectiveness of the system. The audit referred to above may form part of such an assessment.
- The results of the report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be reviewed or modified where necessary.

Designed and Printed by the Government Printing Department - March 2010