Data Protection Office

CODE OF PRACTICE

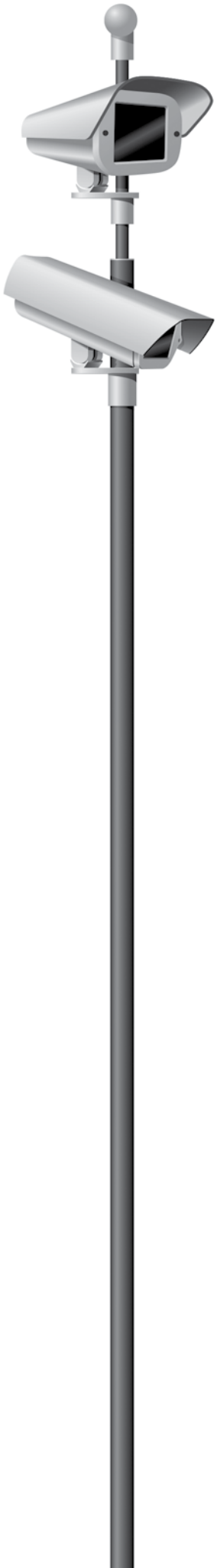
for the operation of the

SAFE CITY SYSTEM(S)

operated by the Mauritius Police Force (MPF)

Issued by the Data Protection Office

Table of Contents



1. INTRODUCTION

The Government of Mauritius envisions to make Mauritius a safer place to live by preventing and reducing criminal activities. In an effort to address these concerns, the Government has introduced the Safe City Project which aims at ensuring the security of citizens and visitors alike.

This Code of Practice sets out the basic conditions for the use of Safe City systems operated by the Mauritius Police Force hereinafter referred to as MPF in accordance with the provisions of the Data Protection Act 2017(DPA). It is the responsibility of the MPF to monitor the compliance of this Code of Practice and to register as a controller with the Data Protection Office. All officers involved in the Safe City system(s) must read, understand and adhere to this Code of Practice.

It is of crucial importance to maintain public confidence in the operation of Safe City systems. Any misuse of these systems is likely to damage the positive perception of the Safe City Project in the eyes of the public. Compliance with this Code of Practice governing Safe City system(s) and their operations will not only assist the MPF to comply with the law but will also help in maintaining the trust of the public in these systems.

2. Definitions

CCTV	Closed Circuit Television
Contract/Service level Agreement	An agreement between the MPF and a processor which outlines the responsibilities of both parties.
Data Protection Act 2017 (DPA)	The law that regulates the processing of personal data about living individuals.
DPO	Data Protection Office
DPP	Director of Public Prosecutions
Controller	a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing (MPF).
Processor	a person who, or public body which, processes personal data on behalf of the MPF.
Data subject	an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Personal data	any information relating to a data subject.

3. Purpose

This Code of Practice has been designed to assist the MPF to operate in accordance with the legal obligations set down in the DPA. It will help MPF ensure that they have in place the operating procedures and protocols necessary to ensure an appropriate use of the Safe City systems, protect against possible misuse and respect the privacy of individuals.

4. Use of the Safe City System(s)

The DPA provides in section 44(1) that:-

No exception to this Act shall be allowed except where it constitutes a necessary and proportionate measure in a democratic society for –

(a) subject to subsection (4), the protection of national security, defence or public security;

(b) the prevention, investigation, detection or prosecution of an offence, including the execution of a penalty;

(c) an objective of general public interest, including an economic or financial interest of the State;

(d) the protection of judicial independence and judicial proceedings;

(e) the protection of a data subject or the rights and freedoms of others; or

(f) issue of any licence, permit or authorisation during the COVID-19 period. (Amended by the Covid-19 (Miscellaneous Provisions) Act 2020)

It is to be noted that the exception of section 44(1)(a) must be read subject to the provisions contained in section 44 (4) of the DPA which stipulates that:

(a) Personal data shall be exempt from any provision of this Act where the non-application of such provision would, in the opinion of the Prime Minister, be required for the purpose of safeguarding national security, defence or public security.

(b) In any proceedings in which the non-application of any provision of this Act on grounds of national security, defence or public security is in question, a certificate under the hand of the Prime Minister certifying that the non-application of the provision is required for the purpose of safeguarding national security, defence or public security shall be conclusive evidence of that fact.

The processing of personal data for the purpose of implementation of the Safe City Project has been exempted through a certificate from the Prime Minister in accordance with section 44(4)(a) of the DPA, from the following sections of the DPA, in the interests of national security, defence and public security:

(a) section 23 (2), (3) and (4) – collection of personal data;

(b) section 26 – communication of personal data breach to data subject;

(c) section 29 but only with respect to personal data pertaining to the commission or alleged commission of an offence by the data subject;

(d) section 37 – right of access;

(e) section 38 – automated individual decision-making; and

(f) section 21, in so far as, it corresponds to the rights provided for in sections 23 (2), (3) and (4), 26, 29 (but only with regard to personal data pertaining to the commission or alleged commission of an offence by the data subject), 37 and 38.

However, the MPF has the duty to comply with the other relevant sections of the DPA.

5. Siting Standards with respect to the Safe City System(s)

- Cameras must be sited in such a way that they only monitor those spaces which are intended to be covered by the system(s).
- Operators must be aware of the purposes for which the scheme has been established.
- Operators must be aware that they may only use the Safe City system(s) in order to achieve the purposes for which the system has been installed.
- Clear and prominent signs must be placed so that the public are aware that they are entering an area which is covered by the Safe City Surveillance 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 Safe City Surveillance System, i.e., the MPF;
    - the purposes of the Safe City Surveillance System;
    - details of who to contact regarding the scheme.
- Operators must also be aware of the position a camera is left in after use. A camera when not in use must be placed in the most advantageous position to record any incidents occurring in a public area within its field of vision.
- Cameras should be situated so that they will capture images relevant to the purpose/s for which the Safe City system(s) has been established.

6. Responsibilities and Accountabilities

- The MPF must at all times ensure the proper and responsible operation of the Safe City system(s) under its control and ensure that all persons operating or monitoring the system(s) are appropriately trained in the systems' use and understand the restrictions and legal obligations imposed upon them by law.
- The MPF shall maintain an appropriate record of the systems' effectiveness.
- It is the responsibility of the MPF to ensure that all uses of the system(s) are appropriate and in the interests of society.
- There must be clear outlined responsibility and accountability for all personal data processed under the Safe City system(s) including images and information collected, held and used. The MPF must establish who has responsibility for the control of this information, for example, deciding what is to be recorded, how the information must be used and to whom it may be disclosed.
- The MPF must be responsible for introducing and implementing the Code of Practice and ensuring compliance with the principles contained within this Code.
- Specific safeguards in respect of the treatment of personal data of vulnerable natural persons such as children must be considered and followed by the MPF.
- The MPF must keep a record of all processing operations under the Safe City system(s).
- The MPF must implement procedures with clearly defined responsibilities for addressing personal data breaches.
- The MPF must notify the DPO without undue delay and, where feasible, not later than 72 hours after having become aware of a personal data breach.
- Where MPF is using the services of a processor for any operations of the Safe City system(s), the MPF must undertake a contract/service level agreement with the processor to ensure that the latter provides sufficient guarantees regarding the security measures they take in relation to the personal data (such as images).
- The MPF must conduct a data protection impact assessment where the processing operations are likely to result in a high risk to the rights and freedoms of the data subjects.
- Where necessary and when the processing is likely to result in a high risk to rights and freedoms of individuals, the MPF must consult the DPO prior to the processing of the personal data.
- A data protection officer/s must be designated by the MPF to be responsible for ensuring compliance with the DPA and this Code of Practice.
- Respect for the individual's liberty and privacy where no criminal offence has been or is being committed should be a primary consideration.

7. Recorded Materials

- The Safe City system(s) must be used fairly and lawfully. Any recorded material must be processed in accordance with the DPA and only for the purposes for which it was established i.e. the protection of national security, defence and public security and to enable the MPF to effectively discharge its duties under the Police Act and such other duties as may be conferred upon it under any other enactment.
- Any recorded material (such as an image, footage, time and date stamps and other identifying materials) must be adequate, accurate, up to date, relevant, and not excessive to fulfil the purposes of the Safe City system(s).

7. 1. Quality of the images/personal information

- Upon installation, an initial check must be undertaken to ensure that all equipment functions properly.
- For any storage media used, it must be ensured that they are of good quality.
- The medium on which the personal information (such as images) has been recorded must not be used when it has become apparent that the quality of information has deteriorated.
- If the system(s) records features such as the location of the camera/person and/or date and time reference, these must be accurate.
- If the system(s) includes location and date/time reference features, users must ensure that they have a documented procedure for ensuring their accuracy.
- Safe City Surveillance System (such as cameras) must be properly maintained and serviced to ensure that clear images are recorded.
- Safe City Surveillance System must be protected from vandalism in order to ensure that they remain in working order.
- A maintenance log of the system(s) must be kept by the MPF.
- If a camera is damaged, there must 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.

7. 2. Security of recorded materials

- Appropriate technical and organisational measures must be implemented to ensure that there is no unauthorised or unlawful processing and accidental loss, destruction or damage of recorded materials.
- All storage media must be stored under lock to which access is restricted to authorised personnel only.
- All storage media held must be counted daily and a record kept by the MPF.
- The MPF must keep an audit log as documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event on the Safe City system(s).
- The recorded materials must be treated according to clear procedures set up by the MPF to ensure continuity of evidence.
- The MPF must ensure that the Safe City system(s) may, in the case of interruption, be restored accordingly.
- The MPF must keep a record or audit trail showing how the information should be handled if it is likely to be used as evidence in Court.

7. 3. Storage and destruction of recorded materials

- Recorded materials must not be retained by the MPF for no longer than is necessary.
- The MPF must establish appropriate time limits for the erasure of personal data and carry out periodic reviews regarding the storage of personal data. Procedural measures must be put in place to ensure that those time limits are observed.
- The MPF must determine the reasonable number of days for which the recorded materials will be erased whenever required and for storage media reuses unless they are required for the investigation of offences or evidential purposes.
- The recorded materials must be stored in a way that maintains the integrity of the information to ensure that the information can be used effectively for its intended purpose.

7. 4. Disclosure of recorded materials to third parties

- Disclosure of the recorded materials to third parties must only be made by the MPF in limited and prescribed circumstances. Circumstances in which disclosure is appropriate must be a lawful requirement under any enactment or Court order to disclose the images with regard to:
    - a formal request from a member of the Police (of at least the rank of Assistant Superintendent of Police), for disclosure of recorded materials, on the grounds that the recorded materials 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 MPF.
- The media, where it is decided that the public's assistance is needed in order to assist in the identification of the victim, witness or perpetrator in relation to a criminal incident. As part of that decision, the wishes of the victim of an incident must be taken into account. The release of recorded materials to the media in a criminal investigation is solely within the remit of the MPF.
    - Note: Where the recorded materials (such as images) are determined to be personal data and it is decided that recorded materials 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.
    - If the system does not have the facilities to carry out that type of editing, an editing company as processor may be hired to carry it out.
- All requests for disclosure must be recorded by the MPF. If disclosure is denied, the reason/s must be documented.
- If disclosure of the images is allowed, then the following must be documented:
    - the date and time on which disclosure was made;
    - the identification of any third party to whom the disclosure was made;
    - the reason for allowing disclosure;
    - the extent of the information which was disclosed;
    - the identity of the officer authorising such disclosure.

8. Police Main Command and Control Centre

- Only person/s authorised by the MPF shall be permitted access to the Police Main Command and Control Centre.
- A register detailing all instances of accesses to the premises must be in place.
- Access to the recorded materials/live footage must be restricted by the MPF to a designated person or persons.
    - Copies of recorded materials must not be made by the MPF. If copies are to be made, the MPF must do so in any of the following circumstances:
        - the incident recorded is of a serious nature (e.g. one that may lead to criminal proceedings);
        - a formal request from the Police (of at least the rank of Assistant Superintendent of Police);
        - the recording is proceeding to trial;
        - a request to view the recording is received from the DPP;
        - the circumstances are such that repeated playing of the incident recorded on is required (i.e. to show to witnesses).

- On removing an extract of the recorded materials, the MPF must ensure that they have documented:
    - the date and time on which the recorded materials were extracted from the Safe City system(s);
    - the name of the person extracting the recorded materials;
    - the reason why the recorded materials were extracted from the system;
    - any crime incident number to which the recorded materials may be relevant;
    - the location of the recorded materials;
    - the name, signature of the collecting official, where appropriate (this includes third parties, the name of the organisation to which the third party belongs).
- All operators and employees having access to recorded materials must be made aware by the MPF of the procedures which need to be followed when accessing the recorded materials.
    - No transfer of any recorded materials must be made to any other authorities outside Mauritius unless there is compelling evidence and it adheres to international binding obligations signed by the Republic of Mauritius and section 36 of the DPA.

9. Rights of the Data Subject

- The MPF must enable an individual to obtain without undue delay
    - rectification of inaccurate or incomplete personal data relating to him or her,
    - erasure of personal data concerning him or her, or
    - restriction of processing of his or her personal data

  on the basis of the conditions provided under the DPA.
- In relation to a request for rectification, erasure or restriction, the MPF must indicate whether it will comply with the request or not.
- The MPF must provide a written response to the individual as soon as reasonably practicable setting out its decision on the request.
- If the MPF decides that the request will not be complied with, it must set out the reasons in its response to the individual.

10. Data Protection Officer

Any queries may be addressed to the Data Protection Officer of the MPF at the following email:

~~ocpior.mpf@govmu.org~~ opsphq.mpf@govmu.org

11. Breaches of the Code of Practice

The MPF has the prime responsibility to investigate any breaches of this Code of Practice and its operations and to remedy the situation to the extent that breaches of the Code are within the legal mandate of MPF's power to remedy.

12. Breaches of Data Protection Act 2017

The MPF is the controller for processing personal data under the Safe City system(s) and must comply with the provisions of the DPA subject to exemptions as provided above.

An individual has the right to lodge a complaint with the Data Protection Office under section 6 of the DPA if he/she considers that the processing of personal data relating to him or her infringes any privacy rights of the DPA.

The complaint may be made in writing to:

The Data Protection Commissioner
Data Protection Office
Level 5, Sicom Tower,
Wall Street,
Ebene Cyber City
Ebene

13. Entry into Operation

This Code of Practice shall come into operation on 30 October 2020.

Design and Print: Government Printing Department © 2020