Marsaxlokk Local Council Surveillance Cameras Policy

This page was intentionally left blank

Table of Contents

This page was intentionally left blank

1. Introduction

In terms of the Local Councils Act (CAP 363) of the Laws of Malta, the Marsaxlokk Local Council (hereinafter referred to as the "Local Council") is a statutory local government authority, hence a public authority under the GDPR, having a distinct legal personality and capable of entering into contracts, of suing and being sued, and of doing all such things and entering into such transactions as are incidental or conducive to the exercise and performance of its functions as are allowed under the Act.

Closed Circuit Television (CCTV) can be a valuable resource in surveillance and security and is widely used by public authorities in a range of premises and situations. However, because of the potentially sensitive nature of surveillance, there are codes, guidelines and legislation which must be complied with in order to operate a CCTV scheme legally and fairly.

Images recorded by a CCTV scheme are deemed to be personal data under the terms of the General Data Protection Regulation (2018). The GDPR applies to **'personal data',** meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

Personal data is not therefore limited to the ability to name an individual. If images of an individual's features are processed and an individual can then be identified from those images, they will amount to Personal Data.

Data is considered to have been processed from the point at which it is recorded and retained, even if the data is not subsequently viewed by anyone.

As with other data, the recorded images from a CCTV scheme may be requested by members of the public in the form of a Subject Access Request within the terms of the General Data Protection Regulation.

All enquiries about and proposals for CCTV installations must in the first instance be directed to the Data Protection Officer.

2. Scope and Purpose

The Local Council deals with personal data by means of CCTV cameras, and as Data Controller, the Local Council is committed to abide by this policy with regards to the data processed by this means.

This Policy identifies the procedures and processes to be followed when planning, implementing and operating a CCTV scheme.

It also provides the reasons and means of processing through the use of a CCTV Surveillance System within the Local Council boundaries whilst ensuring that the rights of the data subjects are not infringed, by processing personal data adequately, not more than necessary and making sure that data is not kept for a period longer than necessary in conformity with legislation and established national procedures established from time to time.

.

3. Legislation

Any CCTV Scheme owned and operated by the Local Council must comply with the following European and/or Maltese legislation:

- The General Data Protection Regulation;
- The Local Councils Act;
- The Data Protection Act;
- The European Convention Act;
- The Freedom of Information Act;
- The Civil Code; and
- Any other legislation that might be established from time to time related to data protection

This Policy must also be read in conjunction with the "Policy Guidelines for the installation and use of CCTV cameras by Local Councils" issued by the Information and Data Protection Commissioner.

In addition, the Local Council shall be duty bound to have regard to any statutory Codes of Practice that might come into force.

4. Responsibilities

All CCTV schemes that process Personal Data as defined by the General Data Protection Regulation 2018 require a "Data Controller" to ensure the correct management of the scheme and the processing of recorded images.

Where a CCTV scheme is run by a business or organisation such as the Local Council, it is the "body" that is the Data Controller rather than an individual member of staff. It is nevertheless important at the very outset to establish who will be responsible on site for all aspects of managing the proposed CCTV scheme on site, to ensure the Council complies with legislation and the statutory Codes of Practice.

In terms of Data Controllers, the Policy Guidelines issued by IDPC state that there are two Data Controllers:

a. The Local Council (Executive Secretaries) shall be the data controllers for processing operations performed by CCTV cameras within their locality.

b. The Police shall be data controllers for copies of video clips/footage forwarded/transmitted to them as a result of detection and prosecution of criminal offences.

If the day-to-day running of the scheme is devolved to someone else, the Data Controller still retains ultimate responsibility for the scheme. The person to whom the running of the scheme is devolved would be committing a criminal offence if s/he were to act outside the instructions of the Data Controller.

If the scheme is devolved to a third party such as a security company, the advice of the Data Protection Officer must be sought.

.

Where two organisations share a scheme, such as a live feed from one scheme to another, and both make decisions regarding its purpose and operation, then they both share responsibility.

The person responsible for the management of the scheme has a number of responsibilities outlined in this policy. Among these is the need to regularly carry out pro-active checks to ensure that this policy is being complied with, including a review of the on-going value and benefit of the scheme. If the scheme is not achieving its purpose it should be discontinued or modified.

5. Point of Contact

There must be a point of contact for members of the public and/or the Local Council employees, which will be identified on signage in the area/s covered by the CCTV camera/s. The point of contact must be available to the public during office hours. Enquirers to the point of contact must be provided on request with one or more of the following:

- This policy
- A subject access request form if required
- Information about the complaints procedure if they have concerns about the use of the system or about non-compliance to this policy.

A record of the number and nature of complaints and enquiries must be maintained together with an outline of the action taken in response. A report of these figures must be produced regularly in order to assess public reaction to and opinion of the scheme.

For the purpose of this policy, the Data Protection Officer shall be the point of contact.

6. Establishing the Need for a CCTV Scheme

While there is a high level of public support for camera surveillance schemes, there are increasing concerns about the role of CCTV in a “surveillance society”. In order to maintain public support and trust, it is important to ensure that the CCTV scheme:

- Is established on a proper legal basis and operated in accordance with the law
- Is necessary to address a pressing need, such as public safety, crime prevention or national security
- Is justified in the circumstances
- Is proportionate to the problem that it is designed to address

A Data Protection Impact Assessment (DPIA) may be required to determine whether the use of CCTV is justified. An assessment should consider the following:

- What is the purpose for using CCTV?
- What are the problems it is meant to address?
- What are the benefits to be gained from its use?
- Can CCTV technology realistically deliver these benefits?
- Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?

.

- Are images of identifiable individuals required, or could the scheme use other images not capable of identifying individuals?
- Could more privacy-friendly options be used instead, such as only recording events likely to cause concern, such as movement in a defined area?
- Will the scheme being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- What are the views of those who will be under surveillance?
- What could be done to minimise intrusion for those that may be monitored, particularly if specific concerns have been expressed?

The Data Protection Impact Assessments (DPIA) shall be carried out using the templates that might be issued by the IDPC from time to time and state how to identify and reduce privacy risks associated with projects such as CCTV surveillance. For this purpose, a risk assessment should be conducted to establish the level of risk, and if this results as "high" further consultations with the IPDC need to be conducted.

7. Establishing the Purpose of a CCTV Scheme

There are four categories for identifying the purpose for CCTV cameras:

i. **Monitoring:** to watch the flow of traffic or the movement of people where it is not necessary to pick out individual figures
ii. **Detecting:** to detect the presence of a person in the image, without needing to see their face
iii. **Recognising:** to recognise somebody who is known, or to determine that somebody is NOT known
iv. **Identifying:** to record high quality facial images which can be used in court to prove someone's identity beyond reasonable doubt.

If the equipment used records sound, this must NOT be used to record conversations between other people, although there are some limited circumstances in which audio recording may be justified, subject to sufficient safeguards. Advice on this can be sought from the Data Protection Officer.

The purpose of the CCTV scheme must be identified and documented, and also the reasons why CCTV is the most appropriate means of meeting the scheme's objectives.

CCTV schemes can be employed for the following purposes:

- Prevention, investigation and/or detection of crime
- Apprehension and/or prosecution of offenders
- Public and employee safety
- Vandalism and illegal dumping
- Traffic management and illegal parking

Once the purpose of the scheme has been identified it is necessary to:

- Ensure that everyone associated with the scheme is fully aware of its declared

.

purpose, and the privacy implications of its use.
- Ensure that the equipment is only used to achieve the declared purpose
- Decide whether constant real time recording is required or whether specific time periods may be more appropriate.

8. Location of the Cameras

The location of the CCTV equipment is very important and must be planned carefully. The physical spaces to be covered must be clearly identified, and the way in which images are recorded must comply with Data Protection Principles as follows:

i. Cameras must only monitor those spaces intended to be covered.
ii. Cameras must be situated to ensure that they will effectively capture images relevant to the scheme's purpose.
iii. If there is a risk of neighbouring spaces being monitored unintentionally the owner of such spaces must be consulted.
iv. Adjustable cameras must be restricted to prevent operators from being able to allow unintended spaces to be overlooked and/or recorded.
v. Cameras must be able to produce images of sufficient size, resolution and frames-per-second
vi. Physical conditions and environment must be borne in mind when siting cameras, for instance taking into account lighting and the size of the area to be viewed.
vii. All necessary steps must be taken to protect the cameras from vandalism and theft.

It should also be noted that some areas have heightened expectations of privacy, such as changing rooms and toilets, and cameras must only be used in most exceptional circumstances to address very serious concerns.

9. Site, justification and purpose of surveillance systems in operation

On the effective date of this policy, the Local Council had the CCTV surveillance schemes installed and operational at:

1 CCTV at Triq tas-Silg, Marsaxlokk, near Chapel
1 CCTV at Triq il-Wilga, Marsaxlokk, Playing Field Area

The sole purpose of surveillance is to ensure security on premises and where necessary in the streets and public facilities cited above for:

- Vandalism
- Security
- Prevention, investigation and/or detection of crime; and
- Apprehension and/or prosecution of offenders.

.

Relevant footage will not be used for any other purpose other than the one intended. Processing for a distinct activity that is not compatible with the original reason for which cameras were installed will only be done if prior notice is given to the data subjects.

In view of Chapter II (Article 5) of the GDPR, the Data Controller justifies the use of a CCTV Surveillance Camera system for the above-mentioned purpose. The recognisable images captured by the cameras will be processed adequately, and in a relevant manner and shall be necessary in relation to the purposes of the processing as per Chapter II Article 6 of the GDPR.

1 Signage

In order to comply with the General Data Protection Regulation, areas covered by CCTV schemes must display signs warning members of the public. The wording and location of signage must take into account the following points:

- Signs must clearly identify to the public when they are entering an area covered by CCTV. These signs can be supplemented with further signs inside the area of required.
- Signs must be clear and legible both in terms of lettering and size, appropriate to the sign's location.
- Signs must identify:
    - Who is responsible for the scheme
    - The scheme's purpose
    - Details of who to contact about the scheme.

In exceptional circumstances it may be agreed that signage may compromise the purpose of the scheme. In such cases it is a must that the Data Protection Officer is informed and provided with the following:

- A specific criminal activity
- The need for CCTV to obtain evidence of that criminal activity
- The reasons why signage would prejudice success in obtaining such evidence.
- How long the monitoring should take place to ensure it is not carried out for longer than necessary.

For ease of reference and display, a sample of a compatible sign is being displayed in Annex 1 to this Policy.

2 Equipment Quality

Procedures and systems must be established to ensure that CCTV equipment is adequately maintained, and that the quality of images recorded consistently meets the purpose of the scheme.

- Recorded pictures and prints as well as live screens must produce good quality images, and the quality must be regularly monitored.

.

- If the system records information such as date, time and camera location, this data must be accurate at all times.
- Equipment must be capable of being set up in such a way as to avoid inadvertent corruption
- If an automatic facial recognition system is used to match images, those images must be of a sufficiently high quality to ensure accurate matching. All matches must in any case be verified and documented by a human operator.
- Selection of equipment must ensure that copies of a recording can be made easily if asked for by a law enforcement agency, and their use of the images should be straightforward.
- A maintenance log must be maintained for all equipment associated with the scheme.
- If a camera is damaged, there must be clear procedures for:

    - Defining who is responsible for ensuring repair/replacement
    - Ensuring the camera is repaired/replaced within a specific time period
    - Ensuring the monitoring and documentation of maintenance work.

3 Data Storage and Access

Retention periods must be established for required and non-required images, and secure and controlled storage and access arrangements for images in compliance with the principles of Data Protection.

For the purpose of this Policy, and in accordance with the guidelines issued by the IDPC on CCTV cameras and Local Councils, the retention period is established in Section 18 of this policy and shall be adhered to unless otherwise requested in terms of the GDPR and national legislation.

In all circumstance, retention periods must be discussed with the Data Protection Officer, and must take into account the following points:

i. Non-required images must be erased as soon as practicable, being permanently deleted through secure methods.
ii. Required images must be retained for a length of time appropriate to their purpose and the purpose of the scheme.
iii. Systematic checks must be carried out to ensure compliance with the agreed retention period.
iv. When the documented period of retention has been reached images must be removed / erased.
v. Any images that are to be retained as evidence must be kept in a secure location with controlled access.
vi. When images are removed for use in legal proceedings the following information must be logged:
    - Date on which images were removed.
    - The reason why they were removed.
    - Any relevant crime incident number.
    - The location of the images.
vii. Signature of the collecting police officer if appropriate.
viii. Monitors displaying images from areas where people would expect privacy must only

.

be capable of being viewed by an authorised employee/s duly approved by the Executive Secretary.

ix. Access to recorded images must be restricted to the designated member of staff responsible for the scheme who will decide whether to allow disclosure to third parties in accordance with the scheme's disclosures policy.

x. Viewing of recorded images must take place in a restricted area with controlled access.

When images are removed for viewing purposes the following information must be logged:

i. Date and time of removal.
ii. Name of person removing the images.
iii. Name/s of the person/s viewing the images. If this includes third parties, it must also include the third party's organisation.
iv. The reason for the viewing.
v. The outcome, if any, of the viewing.
vi. The date and time images were returned to the system or to a secure area.
vii. All operators must be aware of the access procedures that are in place.

4 Disclosure of Images

The Data Controller must ensure that access to, and disclosure of images recorded by the CCTV system is restricted and carefully controlled.

The Data Controller must ensure all employees are aware of the following disclosure and access restrictions:

i. Access to recorded images must be restricted to those who need to have access to achieve the purpose of the CCTV scheme.
ii. All access to images must be logged and documented.
iii. Disclosure of recorded images to third parties must only be made in limited and prescribed circumstances.
iv. All requests for access or disclosure must be recorded. If access or disclosure is denied the reason must be documented.
v. If access or disclosure of images is allowed, then the following information must be logged:
   - The date and time at which access was allowed or the date on which disclosure was made.
   - The reason for allowing access or disclosure.
   - The extent of the information to which access was allowed or which was disclosed.

vi. Recorded images must not be made more widely available. If it is intended that they will be made more widely available that decision must be made by the Executive Secretary or a designated member of staff responsible for the scheme, and the reason for the decision must be documented.
vii. Where images have been disclosed to a third party, then they become the Data Controller for their copy/ies of the image/s and are responsible for compliance with the GDPR.
viii. If images are to be disclosed to the media the images of individuals must be disguised or

.

blurred to ensure that they cannot be readily identified. If the system does not have the facilities for this kind of editing a third party or company can be used. In such cases, the Executive Secretary must ensure that:

- There is a contractual relationship between the Data Controller and the third party or company
- The third party or company has given appropriate guarantees regarding security measures they take
- The Data Controller has checked to ensure that those guarantees are met
- The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the Data Controller or designated member of staff.
- The written contract makes the third part or company's security guarantees explicit.

5 Rights of Data Subjects

Data subjects have a right of access to data being processed as per Chapter II (Article 15) of the General Data Protection Regulation.

6 Access to Footage & Data

Access to the CCTV footage is restricted to authorised personnel only. The Data Controller shall authorise further access to footage if so required when relevant to the purpose/s specified above.

Any criminal activity caught on camera will be disclosed to law enforcement authorities after filing a Police report.

The Local Council undertakes to comply with a strict security policy vis-a-vis the access to recorded images. Any internal access to visual images by the Local Council or any disclosure of such images further to a request by a law enforcement authority or by the data subject shall be logged and kept as evidence.

7 Right of Access

Any individual whose personal data is held by the Local Council, in the form of CCTV recording, can request access to that recording. The Data Controller is obliged to provide access to the footage without disclosing the identity of third parties.

8 Access to Recorded Images by Data Subjects

The Data Controller, including the Executive Secretary and any designated member of staff, must be able to recognise a request from a member of the public for access to recorded images by data subjects.

Data subjects must be provided with a standard subject access request form which will:

.

i. Indicate the information required in order to locate the relevant images.
ii. Indicate the information required in order to identify the person making the request. If the data subject is unknown to the equipment user a photograph of the individual may be requested in order to locate the correct image.
iii. Indicate any administrative fee charged for carrying out the search.
iv. Ask whether the individual would be satisfied with merely viewing the images.
v. Indicate that the response will be provided promptly and in any event within 40 days of receiving the required fee and information.
vi. Explains the rights provided by the General Data Protection Regulation

All subject access requests must be dealt with by the Executive Secretary after consulting the Data Protection Officer, who must also locate the images requested. S/he must also determine whether disclosure to the individual would entail disclosing images of third parties, and whether those third-party images are held under a "duty of confidence".

If third party images are not to be disclosed, the Executive Secretary must arrange for the third-party images to be disguised or blurred. If the system does not have the facilities for this kind of editing a third party or company can be used. In such cases, it is the duty of the Executive Secretary to ensure that:

i. There is a contractual relationship between the Data Controller and the third party or company.
ii. The third party or company has given appropriate guarantees regarding security measures they take.
iii. The Data Controller has checked to ensure that those guarantees are met.
iv. The written contract makes it explicit that the third party or company can only use the images in accordance with the instructions of the responsible member of staff.
v. The written contract makes the third party or company's security guarantees explicit.

If the Executive Secretary decides that a subject request is to be denied, the following information must be logged:

i. The identity of the individual making the request.
ii. The date of the request.
iii. The reason for refusing to supply the requested images.
iv. The name and signature of the person making the decision.

If there is any doubt about whether images are to be disclosed the Data Protection Officer must be consulted.

It should also be noted that in addition to requesting the disclosure of images, individuals also have the right to request notifying the Local Council in writing to cease or to not begin processing images containing Personal Data likely to cause "substantial and unwarranted damage or distress. Advice can be sought from the Data Protection Officer.

If an individual is not satisfied with the reply as provided or with the manner of access that has been granted, the matter may be referred to the Information and Data Protection Commissioner who will investigate the case and ascertain that the right of access is properly granted. Contact details are provided below.

.

18. Retention Period

Personal data is retained for seven calendar days. This period is the necessary period for which the data was obtained.

After the lapse of this period, images are automatically overwritten by new images. If data is extracted in relation to unacceptable behaviour leading to a criminal investigation it will be held for the period required to satisfy said legal claims, and securely erased after such activities are exhausted.

In exceptional circumstance, and as required by the GDPR and national law, the retention period shall be longer than the one established in this Policy. In any circumstances of this nature, the Data Protection Officer is to be informed beforehand.

19. Contact Details

The Data Protection Officer can be contacted on:

Address: Data Protection Officer
c/o Marsaxlokk Local Council
2 Vittorio Cassar Street,
Marsaxlokk MXK 1051
Telephone: +356 7957 3417
Email: DPO@boomconsultancy.eu

The Data Controller can be contacted on:

Address: The Executive Secretary
Marsaxlokk Local Council,
2 Vittorio Cassar Street,
Marsaxlokk MXK 1051
Telephone: +356 2165 2525
Email: marsaxlokk.lc@gov.mt

The Information and Data Protection Commissioner can be contacted on:

Address: Information and Data Protection Commissioner
Level 2, Airways House,
High Street,
Sliema SLM 1549
Telephone: +356 2328 7100
Email: idpc.info@gov.mt

.

20. Approvals and sign offs

This policy comes into effect on 5 June 2019.

Document Control	
Approved By	**Executive Secretary**
Date approved	**24 May 2019**
Next review date	**30 January 2020**

This statement will be reviewed on an ongoing basis. The DPO is responsible for initiating each review.

21. Version control

Version	Date	Changes made by	Details
1.0	20 May 2019	DPO	Surveillance Cameras Policy

.

Annex 1 – Sample of GDPR CCTV Complaint Signage (Section 10)

PUBLIC NOTICE

IN OPERATION

Images are being monitored for the purpose of public safety, vandalism, crime prevention, detection and prosecution of offenders.

Video evidence can be used in a court of law.

This scheme is controlled by
XXXXX Local Council

For further information contact: 21XXXXXX

Read our Surveillance Cameras Policy and/or contact our Data Protection Officer on XXX@xxxx.xxx

.