Kunsill Lokali Ħal Tarxien

CCTV System Policy

Date:

Version Control

Version No.	DATE	CHANGES MADE BY	CHANGES DETAILS
1.0	08/10/2021	DPO	CCTV System Policy

ABOUT THIS POLICY

Kunsill Lokali Ħal Tarxien (hereinafter "the Council") records images (static or video) via a closed circuit television (CCTV) surveillance system (hereinafter "the CCTV System", "CCTV" or "the System") which are installed in the locations stipulated in Annex 1 to this Policy. This CCTV System Surveillance Policy (hereinafter "the Policy") sets out practical guidance on how the Council operates CCTV systems and acquires, retains, processes, and destroys data obtained via such System.

Any recordings made via the CCTV System may include images of persons who appear within the System cameras' vision range. The potentiality that such persons may be identified by the recognition of any distinguishable individual features therefore means that this recording would constitute Personal Data for the purposes of the Data Protection Legislation. Distinguishable features need not only include a person's face, but may also include body shape, general comportment, body marks (such as tattoos or birthmarks), or even items not directly relating to a person's body, such as a vehicle's registration plates or personal accessories.

For all intents and purposes, it must be made clear that the Processing of Personal Data obtained via the CCTV System is considered to be Processed the moment it is recorded and saved (retained) by the Council as delineated in this Policy, and it is not necessary that it is viewed by any member of staff of the Council, or any other authorised or non-authorised person for that matter.

Therefore, Council staff members or any other persons tasked with any action relating to the Processing of Personal Data recorded via the CCTV System, or who in any way handle such Data for whatever reason, must necessarily adhere to the contents of this Policy.

DEFINITIONS

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Legislation. The Council is the Controller of all Personal Data relating to or used by the same Council for the purposes for which it is established by law.

Council: the Kunsill Lokali Ħal Tarxien, established as per the provisions of the Local Government Act (Cap 363 of the Laws of Malta).

Data Subject: a living, identified or identifiable individual about whom the Council holds

Personal Data: Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Protection Legislation (DPL): means (i) unless and until the General Data Protection Regulation (GDPR) is no longer directly applicable in Malta, the General Data Protection Regulation ((EU) 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, in Malta including the Data Protection Act (Ch 586 of the Laws of Malta) and then (ii) any successor legislation to the GDPR or the Data Protection Act (Ch. 586 of the Laws of Malta).

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the Data Protection Legislation.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that the Council can identify (directly or indirectly) from that data alone or in combination with other identifiers the Council possesses or can reasonably access. Personal Data includes Special Categories of Personal Data and pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual

permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Processing (and other grammatical variations thereof) or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

SCOPE & LAWFULNESS

As per Article 3 of the Local Government Act (Cap 363 of the Laws of Malta), the Council is a "*statutory local government authority having a distinct legal personality*" conducive to its carrying out all duties and obligations emanating from the law. By virtue of this distinct legal personality, the Council is therefore falls within the auspices of the General Data Protection Regulation (hereinafter, the "GDPR").

This Policy lays down the necessary procedures to be followed for the proper installation, operation, and use of the Council's CCTV System. The definitions set out in the Council's Data Protection Policy shall be adopted to this Policy. The Policy shall apply to all sections of the Council's entire CCTV System, save where otherwise provided herein. The principles enunciated herein are governed by the provisions of the Data Protection Legislation.

Processing of Data obtained via the CCTV System must always be legitimate and rooted in the allowances provided for in the Data Protection Legislation, as applicable. The Data Protection Principles must therefore be strictly adhered to, and in particular, the following:

- Personal Data Processed must be adequate, relevant, and limited to what is necessary and must be deleted when no longer needed.
- Personal Data must be collected only for specified, explicit and legitimate purposes.
- Personal Data must be Processed in such a manner that its security is guaranteed to the best of the Council's abilities, using appropriate technical and organisational measures to protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- Personal Data must not be transferred to another country which does not abide by the appropriate safeguards or where such safeguards are not in place.
- Personal Data must be made available to Data Subjects, who must be allowed to exercise certain rights in relation to their Personal Data.
- The Council is responsible for compliance with the principles abovementioned.

THE CCTV SYSTEM'S OBJECTIVES

The Council's purposes for installing the CCTV System and Processing the Personal Data recorded by the same shall always be based on the grounds for processing Personal Data, these being the following:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller.

The key objectives of the Council's surveillance systems are:

- To detect, prevent and reduce the incidence of crime or unwanted behaviour;
- To reduce and/or intercept incidences of vandalism and damage;
- To reduce and/or intecept incidences of illegal dumping;
- To enhance the feeling of personal safety and security;
- To enable the identification and subsequent apprehension and prosecution of offenders in relation to crimes actually committed within the proximity of the monitored areas;

- The monitoring and enforcement or traffic related matters

The Council as Data Controller may also be required to process data in compliance with any legal obligation to which it is subject.

Any criminal activity caught on camera will be disclosed to law enforcement authorities after filing a Police report. 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 or if the Council is under a legal obligation to process such data for any such other purpose.

ACCOUNTABILITY & RESPONSIBILITY

The Council is collectively responsible for compliance with the principles abovementioned and shall act as the main Data Controller. Whilst the Council, as an entity, is considered to be the Data Controller for the purposes of this Policy and the Data Protection Legislation, the Executive Secretary shall be the main appointed individual who shall exercise this role and be responsible for the regular operation of the CCTV System and compliance with this Policy. On its part, the Data Protection Officer shall relay any necessary advice regarding the implementation and observance of this Policy.

Any queries on this Policy and its application may be directed to the DPO via the following email address: dataprotection.tarxien@gov,mt. The DPO shall maintain a register of any such queries or complaints made with reference to this Policy or the matters which it addressed. Such register, its contents, and an explanation thereof must be ready for presentation at any given time. Furthermore, a data subject has the right to complain to the Data Protection Commissioner about the Council's processing activities using the following contact details:

Office of the Information and Data Protection Commissioner
Floor 2,
Airways House,
Hight Street
Sliema SLM 1549
Phone: (+356)23287100

Access to the recordings obtained via the CCTV System shall only be permitted to Executive Secretary. The recordings shall be stored in [LOCATION]. The Council will do its utmost to ensure that only persons so authorised may access and view the footage described herein.

Since most CCTV System recordings constitute the processing of Data on a fairly large and public scale, the Council shall regularly conduct a Data Protection Impact Assessment ("DPIA") in relation to it. Any Data collected shall be processed strictly within the parameters of the purposes stipulated in this Policy. Such Data will not be used for any commercial or marketing purposes at any point.

LOCATIONS OF CCTV SYSTEM CAMERAS

As at the date of the adopting of this Policy, the Council has installed a total of _____CCTV Systems located at the following monitored areas:

INDICATE NUMBER & TYPE OF CAMERAS, AND REASON BASED ON THE ABOVE].

RETENTION OF DATA

Unless required for evidential purposes, the investigation of an offence or as required by law, Personal Data recorded via the CCTV System shall, by default, be kept for no longer than 7 days from the date and time of recording. Where CCTV footage is required to be held in excess of the retention period referred to herein, the reason therefor will also be explained. CCTV footage held in excess of their retention period will be reviewed on a 3 monthly basis and any footage not required for evidential purposes will be deleted.

Any retention periods for Data collected for purposes other than those already provided for in this Policy shall be discussed with the DPO, taking into account the period proposed, whether it is reasonable for the aim being pursued, and the proposed duration of the implementation of this purpose, if any.

The table below indicates the type of Data being collected and in what manner (Data Surveillance Type), the location of the respective instrument (Location) and the retention period of the Data being collected through it (Retention):

Data Surveillance Type	Location	Retention
X	X	X

SIGNAGE

In any site which falls within the vision range of any CCTV System camera, adequate signage must be displayed in prominent locations with sizeable, clear and legible wording, which can be easily viewed by anyone entering the area, particularly in sections where one will certainly be caught in the System's vision range. Special consideration must be made as to the adequacy of the size and display of signs within open, public spaces. Signs must be regularly maintained, particularly those which are in place in the outdoors, to ensure that they are up to standard and the content thereof is still visible.

What must the signs include?

- A warning that the CCTV System is operating and recording footage within the area it is located
- The point of contact and person responsible for any issues related to the CCTV System and the footage recorded, who shall be Executive Secretary
- What the CCTV System aims to achieve (i.e. the legal basis for processing)
- The times and days during which the footage is being recorded (even if 24/7)
- The retention period of the footage

DATA REPOSITORY

Responsibility and ownership of the data obtained through the CCTV System shall lie with the Council. All data so obtained shall be kept [EXPLAIN STORAGE SYSTEMS& LOCATION].

DATA SECURITY MEASURES

The Council shall implement all necessary technical and organisational security measures to protect the CCTV System itself and all the footage (Personal Data) which is recorded thereby, taking into account the nature, scope, context, and purposes of the Data being Processed together with any underlying risks to which the Data may be exposed at any given time, most especially in terms of the risks posed upon the rights and freedoms of the Data Subjects. Sufficient safeguards must also be implemented to ensure the avoidance of any unauthorised, unlawful or accidental loss, damage, alteration, disclosure, transmission, erasure or destruction of any Data recorded by the CCTV System.

The Council shall ascertain that all employees and other authorised persons who view, access or otherwise handle the Data collected by the CCTV System in accordance with this Policy are aware of the security measures mentioned herein.

ACCESS TO SYSTEM DATA

Access to the recordings shall be solely limited to the Executive Secretary and the DPO. A log of each time Data recorded by the CCTV System is accessed shall be kept by the Controller. Any person wishing to obtain access to any Data recorded in this manner must obtain permission from the Executive Secretary to do so. When any person accesses footage so recorded within its legitimate retention period as per this Policy, the Controller must record the date, time and reason of access, by whom the Data was accessed, and conclusions or other remarks drawn from such access.

In the case that such access consists of the need to disclose Data recorded via the CCTV System to third parties other than the persons authorised by this Policy (whether autonomously or upon request), such as the Executive Police, this fact must also be recorded in the log mentioned above, together with the identity of the person/s to whom access is granted and the reason for this.

In the case that a request for access by a third party is made but such request is denied, the details of the request must nonetheless be recorded and the reason for the refusal to access also explained.

If any Data recorded via the CCTV System must be published for some legitimate reason or other, this shall also be noted in the manner discussed above. The Executive Secretary shall ensure that every effort is made to anonymise any such data by blurring out persons appearing in the footage and making them unrecognisable both in terms of facial recognition and other unique traits, such as build or characteristics, so long as there are no legitimate grounds for any individual appearing in the footage to not be anonymised in any given case.

All Council employees and other persons are hereby being made aware that access to the Data recorded by the CCTV System as held by the Council is not permitted unless such employee or other person is directly authorised to access it by this Policy or by a direct order in writing by Executive Secretary.

TEMPORARY SYSTEMS

As specified in this Policy, oftentimes CCTV System arrangements may be made for the installation of cameras or other recording devices forming part of the CCTV system in specific circumstances, such as for the prevention or detection of criminal activity upon reasonable suspicion thereof. In such cases, temporary CCTV System installations may be made in areas where such installations are not available.

A log of all temporary CCTV System installations will be kept and retained by the Executive Secretary, together with a description thereof, the date and time of installation, the retention periods of any data collected via such temporary installations, together with the proposed date for its removal. The Executive Secretary must approve such installations, and such authorisation must be reviewed every 6 months.

Any extensions to the proposed date of removal must furthermore be approved by the Executive Secretary, which proposal shall be noted in this log together with the reasons supporting the decision for approval or rejection, and the new established removal date.

SYSTEM MAINTENANCE

The Council shall ensure that all parts making up the CCTV System are regularly checked and maintained in order to ensure footage of an acceptable quality and with a reasonable degree of accuracy both in terms of image quality and ancillary recorded details, such as date and recording time. All CCTV System installations shall be positioned and installed in such a way that eliminates the risk of tampering or other unauthorised access.

A log of all regular (planned) and irregular maintenance, including response to reports of damage, exercises carried out shall be kept by the Executive Secretary, highlighting who was responsible for the maintenance (in the case of an external third party entity, both the name of the entity and the person responsible for the maintenance must be noted), the date and time of maintenance, and a brief outline of what work was carried out, and whether it was routine or unplanned.

DATA SUBJECT ACCESS

Any Data Subject who believes that the Council holds any Personal Data relating to him/her as recorded by the CCTV System may submit a Data Subject Access Request as per the Council's Data Subject Access Request Policy, which policy shall be made available to any person requesting such Data, together with the relevant request form. For further information on this, please refer to the Data Subject Access Request Policy.

The Council shall provide any Data relating to the Data Subject making such a request within the parameters it deems feasible. The Council shall furthermore reserve the right to refuse to provide any such Data if it has reasonable grounds to do so, such as the impossibility or anonymising any other Data Subjects who appear within the same footage being requested. Should a third party entity be tasked with such an anonymisation exercise in the case that the Council does not have the facilities to effect this itself, the Council shall ensure compliance with data sharing principles on the basis of a contractual data sharing agreement, as previously indicated in this Policy.

DATA CONTROLLER AND DATA PROTECTION OFFICER CONTACT

Should you wish to contact the Data Controller or the Data Protection Officer for any reason related to this Policy, you may do so here:

Kunsill Lokali Ħal Tarxien 73 Triq Santa Marija , Tarxien Malta TXN 1704
+356 21 666 688
tarxien.lc@gov.mt

Ongoing Review of CCTV Use

The Council will ensure that the ongoing use of existing CCTV cameras in the monitored areas is reviewed periodically to ensure that their use remains necessary and appropriate and whether or not such surveillance systems continue to address the needs that justified their introduction.

POLICY REVIEW

The Council's usage of CCTV and the content of this Policy shall be reviewed annually by the Data Controller with reference to the relevant legislation or guidance in effect at the time. Further reviews will take place as required.