

## CCTV SURVEILLANCE CAMERAS POLICY FOR AĠENZIJA SAPPOR

### Scope

The Aġenzija Sappor deals with personal data by means of CCTV cameras and abides by this policy with regards to the data processed by this means.

### Background Information

The data controller for Aġenzija Sappor is the Chief Executive Officer.

The data protection officer representing Aġenzija Sappor may be contacted as follows:

### Address

Aġenzija Sappor, Triq il-Harrub Santa Venera SVP 9018

### Telephone

(+356) 2256 8000

### Email

[gdpr.sappor@gov.mt](mailto:gdpr.sappor@gov.mt)

Data subjects will have a right of access to data being processed as per Chapter II (Article 15) of the General Data Protection Regulation. (Please refer to section relating to Access, below). Data subjects are also hereby informed of their right to object to the processing of their personal data and to lodge a complaint with the Information and Data Protection Commissioner.

The Information and Data Protection Commissioner may be contacted as follows:

**Address**

Information and Data Protection Commissioner  
Level 2, Airways House  
High Street  
Sliema SLM 1549  
Malta

**Telephone**

(+356) 2328 7100

**Email**

[idpc.info@gov.mt](mailto:idpc.info@gov.mt)

**Location & Purpose**

CCTV surveillance is installed in Aġenzija Sapport's offices, residences and day centres i.e. total of 25 CCTV cameras installed as follows: 3 in parking lots, 8 back doors/emergency doors/ 8 reception area's/ 4 front doors/ 1 entrance to lift and 1 in archives room. Affixed notices are placed in prominent and easily visible places within the monitored area.

The purposes of surveillance are:

- i. for the security of Aġenzija Sapport's premises, property, and the security of it's employees, service users and visitors.
- ii. for the establishment of relevant facts in the case allegations of the commission of a serious disciplinary offence or criminal offence are made regarding any employee which would merit further investigation in terms of Aġenzija Sapport's disciplinary policy.
- iii. for use as evidence in any disciplinary proceedings relating to the commission of a serious disciplinary offence by any employee, or in any criminal investigation or proceedings either upon

a request from any competent law enforcement or regulatory authority or which may be furnished by Aġenzija Sapport as it deems necessary in order to prevent, disclose or detect the commission of acts that amount or are likely to amount to a criminal offence or gross misconduct on the part of any employee.

Relevant footage will not be used for any other purpose other than the one intended. More specifically, relevant footage will not be used to monitor employee activity, save as provided for above. 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 Article 6 of the GDPR , the Data Controller justifies the use of a CCTV Surveillance Camera system for the above-mentioned purpose on the basis of its legitimate interest to ensure that (i) it's premises are adequately monitored and the security of its premises, property, employees, service users and visitors is safeguarded at all times; (ii) it can effectively investigate any allegations of serious misconduct on the part of any employee and effectively enforce its disciplinary procedures in case of a breach; and (iii) to prevent or disclose the commission of any criminal offence. The Data Controller may also be required to process data in compliance with any legal obligation to which it is subject. The recognisable images captured by the cameras will be processed in accordance with good principles of processing of personal data as required in terms of Article 5 of the GDPR.

### **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.

Aġenzija Sapport may be required to allow access to the CCTV footage or to provide copies of such footage upon an official request by the Police or other authority which may be authorised by law to request such footage.

Aġenzija Sapport undertakes to comply with a strict security policy vis-a-vis the access to recorded images. Any internal access to visual images by Aġenzija Sapport 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.

## **Right of Access**

Any individual whose personal data is held by Aġenzija Sapport 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.

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.

Right of access request shall be made in writing and addressed to the Controller.

## **Retention Period**

Personal data is retained for 31 days maximum where applicable, which period is the necessary period for Aġenzija Sapport to effectively achieve the purposes for which the data was obtained. After the lapse of this period, images are automatically deleted/ overwritten by new images. If data is extracted in relation to unacceptable behaviour leading to a criminal investigation or upon an official request, it will be held for the period required to satisfy said legal claims, and securely erased after such activities are exhausted.

## **Conclusion**

This policy provides the reasons and means of processing through the use of a CCTV Surveillance System within Aġenzija Sapport 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 Data Protection Legislation.

*Version: 01.2018*