

CCTV Surveillance Cameras Policy for CRPD

Scope

CRPD deals with personal data by means of CCTV camera/s and abides by this policy with regards to the data processed by this means.

Background Information

The data controller for CRPD is the Commissioner for the Rights of Persons with Disability.

The data protection officer representing the Commissioner for the Rights of Persons with Disability may be contacted as follows:

ADDRESS

CRPD
G5 Offices
Psaila Street,
Birkirkara BKR 9077

Telephone

(+356) 22267600

Email

Datacontroller@crpd.org.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 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@idpc.org.mt

Location & Purpose

CCTV surveillance is installed in CRPD's premises, i.e on the ground floor including its entrance, the first floor, the second floor and the basement/garage including its entrance. Affixed notices are placed in prominent and easily visible places within the monitored area. The sole purpose of surveillance is to ensure security. 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.

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.

CRPD undertakes to comply with a strict security policy vis-a-vis the access to recorded images. Any internal access to visual images by CRPD 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 CRPD, 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 a period of seven days. This period is the necessary period for which the data was obtained. After the lapse of this period, images are 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.

Conclusion

This policy provides the reasons and means of processing through the use of a CCTV Surveillance System within CRPD 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.

Date: April 2020