LIMERICK
TWENTY
THIRTY DAC

Limerick Twenty Thirty DAC

CCTV Data Protection Policy 2019

AUTHOR: DENIS O SULLIVAN

ADVANCE SERVICES FACILITIES MANAGEMENT (ASFM)

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

The purpose of this policy is to address the data protection issues associated with having Closed Circuit Television (CCTV) on the premises of Limerick Twenty Thirty DAC, The Mercantile, Gardens International, Henry Street, Limerick (hereafter referred to as LTT). The system comprises of 5 cameras.

The purposes for installing CCTV is to ensure the security of premises, staff, aiding in the prevention and detection of theft and other crimes, The Safety Health and Welfare at work act 2005.

The cameras are fully operational and are Dome type. The system is operated from a control room located in a comms room in the Main Gardens International Building. This room is secured with swipe access control by authorised personnel.

Cushman & Wakefield the property management company are responsible for the management and maintenance of the CCTV system for (LTT) this Includes following and adhering to the (LTT) CCTV policy including all access requests, documentation, and records.

Cushman & Wakefield are also responsible for management and maintenance of the CCTV system for the Gardens International Building which includes the 4 listed cameras for LTT (as listed in section 3.2) in addition Cushman & Wakefield have responsibility for all external cameras which fall under Gardens International.

SECTION 2: POLICY

Policy Statement

Data Protection Legislation applies as CCTV recordings can include personal data. CCTV is regulated in accordance with the Data Protection Acts 1988, 2003 & 2018, and by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and guidelines issued by the Office of the Data Protection Commission (Guidance on use of CCTV for Data Controllers) updated May 2019. Code of Practice for CCTV Systems authorised under Section 38(3)(c), of the Garda Síochána Act 2005, (hereafter referred to as the Garda Code of Practice).

This Policy will be kept under review with regard to the system meeting its purposes.

Policy Purpose

The purpose of this Policy is to provide guidelines to regulate the management, operation, access and use of the CCTV systems and resulting images at the Mercantile Building occupied by LTT in a way that enhances security whilst respecting the expectation of reasonable privacy among members of the public, staff, and visitors.

CCTV surveillance at the LTT office is intended for the purposes of:

- Protecting the building and assets, both during and after office hours;
- Promoting the health and safety of staff, and others.
- Monitoring issues relating to public access such as removal of documents;

Policy Scope

This policy applies to all locations within the Mercantile Office building occupied by (LTT).

The CCTV systems will not be used for any other purposes than outlined, for example, CCTV will not be used to monitor the work of employees or monitor attendance.

There are CCTV systems installed on a number of locations within the Gardens International facility internal and external where (LTT) is not the lead tenant in the building. In such case, (LTT) is NOT responsible for these CCTV systems and they are outside the scope of this Policy. The property management company Cushman & Wakefield is responsible for these CCTV systems.

SECTION 3: LAWFULLNESS AND TRANSPARENCY OF PROCESSING

The fair obtaining principles inherent in data protection legislation, require that those people whose images may be captured on camera are informed by having adequate signage in place at the Mercantile Building occupied by (LTT).

Adequate signage will be placed at each location in (LTT) where CCTV cameras are situated to indicate that CCTV is in operation (locations listed below).

As well as this, the LTT Data Protection Officer will provide a copy of this CCTV Policy to (LTT) staff and on request to visitors to LTT Offices at the Mercantile Building.

The CCTV Policy is made available also in the Data Protection Statement on the Limerick Twenty Thirty website.

3.1 Principles relating to processing of personal data as set out in (Article 5 GDPR)

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

3.2 Location of Cameras

CCTV Cameras are located in the following locations:

Camera Location	Camera Number	Camera Type
Stairs 5 – Ground Floor Entrance	19	Dome
Stairs 5 – 1st Floor	36	Dome
Stairs 6 – Ground Floor Entrance	23	Dome
Stairs 6 – 1st Floor	41	Dome
Ground rear exit lane	22	

Video monitoring of public areas for security purposes is limited to uses that do not violate the individual's reasonable expectation to privacy and this is managed by (Cushman & Wakefield) the property manager.

3.3 NOTIFICATION – SIGNAGE

A copy of this CCTV Policy is available to staff and at reception for contractors and visitors to the office on request. This policy describes the purpose and location of CCTV monitoring, a contact number for those wishing to discuss CCTV monitoring and guidelines for its use. Adequate signage is placed at each location in which a CCTV camera is sited to indicate that CCTV is in operation. Signage shall include the name and contact details of the data controller.

SECTION 4: OPERATION OF THE CCTV SYSTEM

The system can only be accessed by authorised personnel acting for and on behalf of (LTT). The property management company (Cushman and Wakefield) have overall responsibility.

The contract between the property management company (Cushman & Wakefield) and the CCTV service company stipulates the security standards as set out in this document.

The system is housed in a secure, locked room, which is accessible to authorised personal only and the CCTV system is password protected with varied levels of control.

Article 5.1.f of the GDPR states that personal data collected shall be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures, to protect it from:

- Unauthorised or unlawful processing
- Accidental Loss
- Disclosure
- Destruction

This is the principle of integrity and confidentiality.

All precautions are taken by (LTT) to prevent unauthorised people from having access to view, copy or interfere with CCTV footage. Access is restricted to authorised personnel only. The CCTV system is password protected with each authorised user having their own named login.

Cushman & Wakefield will keep a written log of who accesses the CCTV system to view images, including Gardaí viewing it to see if it contains material relevant to a criminal investigation.

SECTION 5: DATA PROTECTION, STORAGE AND RETENTION

The data captured from the CCTV cameras is securely stored as electronic data. Typically, this data is recorded and will be retained for maximum of 28 days. It will be over-written after that period. However, data may be retained for longer period's e.g. (65 days in the case of a personal injury) or where the events captured give rise to court proceedings. Access to the data is restricted to authorised personnel.

So, anything which makes another individual identifiable: faces, distinctive clothing or identifying features of vehicles, such as registration numbers, roof racks or unusual hubcaps must be pixelated or redacted.

The storage devices are password protected. Supervising the access and maintenance of the CCTV system is the responsibility of (Cushman & Wakefield). Unauthorised access will be viewed as a data breach.

Section 6: RETENTION OF IDENTIFIABLE IMAGES

On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release. In fulfilling these requests (LTT) cannot release the identifiable images of other data subjects, so anything which makes another individual identifiable: faces, distinctive clothing or identifying features of vehicles, such as registration numbers, roof racks or unusual hubcaps must be pixelated or may only be released where they can be redacted / anonymised so that the other person is not identified or identifiable.

SECTION 7. ACCESS REQUESTS

In relevant circumstances, CCTV footage may be accessed:

• By An Garda Síochána, where LTT is required by law to make a report regarding suspected crime;

- An Garda Síochána may wish to view CCTV footage to see if it is of assistance. Where An Garda Síochána view the footage on (LTT) premises or that of an (LTT) Processor, no data protection concerns arise.
- Where An Garda Síochána request to view CCTV in public areas when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place or within the Main Gardens International building then the request must be made to Cushman & Wakefield following the Cushman & Wakefield CCTV Policy.
- To Data Subjects (or their legal representatives) in response to an access request for cottage of CCTV within the Mercantile building (LTT) where the time, date and location of the recordings is furnished to LTT;
- To individuals (or their legal representatives) subject to a court order;
- To the LTT insurance company where the insurance company requires the same in order to pursue a claim for damage done to the insured property.

7.1 ACCESS REQUESTS BY AN GARDA SÍOCHÁNA

In line with Data Protection legislation, An Garda Síochána are entitled to view personal data on individuals, if it is for the following purposes;

- For the prevention and detection of crime
- For the prosecution of offenders
- When required urgently to prevent injury or other damage to welfare of the person or serious loss or damage to property
- When required under an order of the court or any other enactment.

With regard to requests from An Garda Síochána to download footage, the Data Protection Commission recommends that requests for copies of CCTV footage should only be granted when a formal written request is provided to (LTT) stating that An Garda Síochána is investigating a criminal matter.

For practical purposes, and to accelerate response to an urgent request, a verbal request may be adequate to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request.

A log of all An Garda Síochána requests will be maintained by (LTT) and its data processors. Any such requests should be on An Garda Síochána headed paper, signed by a superior officer quoting the details of the CCTV footage required and should also quote the legal basis for the request under the data protection legislation.

Prior to (LTT) issuing any CCTV images to An Garda Síochána, it will be discussed and agreed with LTT(s) data protection officer.

7.2 PROVIDING ACCESS TO CCTV TO DATA SUBJECTS (THIRD PARTIES)

Any person whose image has been captured on a (LTT)CCTV system as outlined in this document has a right to be given a copy of the information recorded, providing that such an image/recording exists (i.e. That it has not been deleted). To exercise that right, a person must make an application in writing to (LTT) and provide proof of identity, and proof of address, giving a reasonable indication of the time period sought, and identifying the location of the camera. If the person is under eighteen years, the parent or guardian may make an application. Access requests must be responded to by (LTT) within one month (30 days) of receipt

In giving a person(s) a copy of their data LTT may provide video, or where footage is technically incapable of being copied to another device or in exceptional circumstances it may be acceptable to provide still/series of still pictures with relevant images as an alternative to video footage for the duration of the recording in which the requester's image appears to comply with our obligation to supply all personal data held.

Where images of parties other than the requesting data subject appears on CCTV footage then (LTT) will pixelate or may only be released where they can be redacted / anonymised so that the other person is not identified or identifiable before supplying a copy from the footage to the requester.

APPENDIX 1: DEFINITIONS

SUBJECT ACCESS REQUEST (SAR) – this is where a person makes a request to the organisation for the disclosure of their personal data held by the psi under the applicable data protection legislation.

CLOSED CIRCUIT TELEVISION (CCTV) – is the use of video cameras to transmit a signal to a specific place on a set of monitors, generally for security purposes. The images may then be recorded on video tape or DVD or other digital recording mechanism.

THE GENERAL DATA PROTECTION REGULATION AND DATA PROTECTION ACTS 1988-2018 - data protection legislation confer rights on individuals as well as responsibilities on those persons processing personal data. All staff must comply with the provisions of the data protection legislation when collecting, storing, sharing, or otherwise processing, personal information. This applies to personal information relating both to personnel of the organisation and individuals who interact with the organisation.

DATA - includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer.

PERSONAL DATA – data (information) relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

DATA BREACH - any event which results in the integrity or security of personal data being compromised. It can include loss or theft of electronic equipment on which personal data is stored, equipment failure, human error, loss or sharing of information, or a cyberattack, accidental loss of personal data (e.g. fire and flood).

DATA CONTROLLER - a person who (either alone or with others) controls the contents and use of personal data.

DATA PROCESSING - processing covers a wide range of operations performed on personal data, including by manual or automated means. It includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.

DATA PROCESSOR - is a person or organization who deals with personal data as instructed by a controller for specific purposes and services offered to the controller that involve personal data processing this might mean an employee of an organisation to which the data controller out-sources work. Processor means a natural or legal person, public authority, agency or other body which processes personal data.

DATA SUBJECT – an individual who is the subject of personal data.