CCTV (Closed Circuit Television System)

Standard Operating Procedure

Summary of Contents

In compliance with relevant local laws, this Standard Operating Procedure (SOP) provides staff, contractors, guests and visitors with information, guidance and procedures in relation to the company's use of CCTV and its disclosure within controlled conditions.

Date of this issue: 3 June 2020
AREA: Global
Responsible Owner: Information Security Manager

Review Information

Created: June 2020
Reviewed: Next Review Due : June 2021

1 INTRODUCTION AND PURPOSE

1.1 citizenM Operations Holding BV ("us" or "we") operates a Closed-Circuit Television system ("CCTV") in all hotels, to view and record individuals – specifically all staff and contractors at, and guests and visitors to, premises owned, leased or managed by us.

1.2 We believe that the use of CCTV has a legitimate role in helping to maintain a safe and secure environment for all staff, contractors, guests and visitors to our premises, and to protect our property against criminal damage.

1.3 However, we also recognise that our use of CCTV may raise privacy concerns. Images of individuals and/or images relating to them recorded by our CCTV constitutes 'personal data' under relevant data protection legislation.

1.4 citizenM is registered with the relevant supervisory authorities to process personal data, to the extent such registrations are required under applicable data protection legislation.

1.5 The purpose of this Standard Operating Procedure ("Procedure") is to outline citizenM's approach to using CCTV and to ensure that we comply with our obligations under relevant data protection legislation when recording and using CCTV images.

1.6 This Procedure outlines why and how we use CCTV; how we process personal data recorded by CCTV; and how we handle subject access requests made in respect of personal data recorded by CCTV.

2 SCOPE

2.1 This Procedure applies to all citizenM staff (including contractors and temporary staff) ("you") who have access to, responsibility for, or may otherwise use our CCTV.

2.2 All such individuals must help us to comply with our data protection obligations by only using CCTV in accordance with this Procedure.

2.3 All CCTV imagery is automatically recorded, and any breach of this Procedure will be detected via controlled access to the system and auditing of the system.

2.4 Any failure to comply with this Procedure may be a disciplinary offence which could result in dismissal. Negligent or deliberate breaches of this Procedure or misuse of CCTV could result in criminal liability for you personally.

2.5 This Procedure does not apply to targeted surveillance activity.

3 RESPONSIBILITY FOR COMPLIANCE

3.1 Our Information Security Manager is the primary contact for CCTV and is responsible for day-to-day compliance with the requirements of this Procedure.

3.2 The Information Security Manager is also responsible for deciding, in accordance with the terms of this Procedure, what is to be recorded by our CCTV cameras, how the recordings should be used; and to whom the recordings may be disclosed.

3.3 If you have any queries about this Procedure, please contact privacy@citizenm.com.

4 WHY WE USE CCTV

4.1 We only use CCTV for specified purposes in pursuit of a legitimate aim and where such use is necessary to meet an identified pressing need.

4.2 We currently use CCTV on our premises as we believe that such use is necessary for the following legitimate business purposes:

a) to prevent, act as a deterrent against and detect crime and disorder;

b) to protect our buildings, equipment and assets from damage, disruption, vandalism and other crime;

c) for the personal safety of staff, contractors, guests and visitors to our premises and other members of the public;

d) to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings;

e) to support law enforcement bodies in the prevention, apprehension, detection and prosecution of crime (including use of recordings of the premises and its immediate surroundings as evidence in criminal proceedings); and

f) in exceptional circumstances (and with explicit permission from Human Resources), to assist in the defence of any civil litigation, including employment tribunal proceedings.

4.3 Other purposes may be or become relevant in future but before using CCTV for an additional purpose we will always carry out a data protection impact assessment to consider the effects of CCTV on individuals and their privacy and balance this against the legitimate interest being pursued.

5 HOW WE USE CCTV

5.1 The CCTV system operates 24 hours a day, 7 days a week, and records to digital recording media. These cameras are currently monitored on the premises.

5.2 We own all images captured on our CCTV surveillance systems.

5.3 We comply with the provisions below regarding how we position and signpost our CCTV cameras and how we ensure the quality and appropriate storage of the recordings they capture.

Siting the Cameras

5.4 The information recorded by our CCTV cameras needs to be adequate for the purposes set out in section 4.2 above. As such, it is vital that they are positioned appropriately. The positioning of our CCTV cameras is also critical to ensuring our compliance with data protection legislation.

5.5 At present, we have CCTV cameras covering various entrance and exit points throughout buildings owned, leased or managed by citizenM, and in some premises there are cameras on all floors (excluding inside guests' rooms, changing rooms, staffrooms or toilet areas).

5.6 The following principles were followed by us in positioning those cameras. The Information Security Manager will ensure that these principles are followed if, in the future, we propose to install new cameras or change the positioning of any existing cameras at any of our premises:

a) Cameras should be restricted to monitor only those areas which are intended to be monitored and should not view any areas that are not of interest / are not intended to be the subject of surveillance. Where cameras are adjustable, they should be restricted so that they cannot be adjusted to overlook areas outside the CCTV monitored site. Cameras should not film employees at their work stations, except in special circumstances. Cameras must also not film employees' breakroom, toilets or rest areas. Finally, they must not film union offices or staff representatives, nor their access when it leads to these offices;

b) Cameras should not be used to monitor any adjoining areas which are not intended to be covered by CCTV and must not be sited in private places, such as guests' rooms, changing rooms, staffrooms or toilet areas; and

c) Cameras should be positioned to record images which are relevant to the purposes for which we use them and to produce images of the right quality (bearing in mind the technical capabilities of the camera, the environmental factors, the lighting and the size of the area to be viewed by the camera).

Signposting the cameras

5.7 We aim to be as transparent as possible about our use of CCTV cameras. Data protection legislation requires us to notify individuals if they are in an area where CCTV surveillance is being carried out.

5.8 We have erected signs on all entrance points to all buildings owned, leased or managed by us to ensure citizenM staff, contractors, guests and visitors are aware they are entering an area that is covered by CCTV cameras.

5.9 All our signs:

a) alert individuals that they are entering a CCTV monitored zone;

b) are legible and visible (the size of the sign will depend on the location and how visible it is to individuals);

c) are positioned at a reasonable distance from the places monitored in such a way that individuals can easily recognise the circumstances of the surveillance before entering the monitored area (approximately at eye level). Individuals must be able to estimate which

area is captured by a camera so that they are able to avoid surveillance or adapt their behaviour if necessary; and

d) specify that CCTV is operated by citizenM Operations Holding BV and provide a phone number and/or email address where individuals can obtain further information.

Quality of recordings

5.10 CCTV recordings must be suitable for the purposes described in section 4.2 of this Procedure. For example, as we may use CCTV recordings for crime detection and prevention purposes the images must be clear enough to identify individuals and be used in evidence.

5.11 Equally, however, our CCTV cameras should not capture more data than is necessary in order to fulfil the purposes in section 4.2.

5.12 To ensure and maintain the quality of our CCTV recordings, we do the following:

a) Upon installation all CCTV equipment must be tested to ensure that only the designated areas are monitored, and high-quality pictures are available in live and play back mode;

b) CCTV equipment is serviced annually and must be checked, maintained and cleaned regularly to ensure it functions properly and clear, good quality images are recorded. The date and time on the CCTV cameras should also be periodically checked to ensure they are accurate; and

c) We must ensure all relevant software updates are applied in accordance with the system manufacturer's instructions.

Storing recordings

5.13 While CCTV recordings are retained, it is essential that their integrity be maintained (whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded).

5.14 As such, our CCTV recordings must be stored on a secure medium and in a secure place to which access is controlled (this is particularly important where images may be used for evidentiary purposes). To ensure that we meet our security obligations we ensure that:

a) control rooms and areas where CCTV recordings are stored are kept secure at all times and locked when unoccupied; and

b) access to the CCTV recordings is restricted to authorised staff only;

c) the Information Security Manager (or a person nominated to act on their behalf) controls viewing of images on the premises;

d) staff are given appropriate training regarding CCTV and the requirements of this Procedure and are made aware that misuse can be a criminal offence; and

e) disclosure of CCTV recordings (where permitted in accordance with this Procedure) is undertaken using a secure method of transmission or delivery (to minimise the risk of recordings getting lost in transit or being intercepted).

6 RETENTION AND DISPOSAL OF CCTV RECORDINGS

6.1 Relevant data protection legislation prevents us from keeping CCTV recordings for longer than necessary for the purposes set out in section 4.2 above. We have, therefore, established that all CCTV recordings will be retained for a maximum of 30 days, unless we are made known of images which may assist with an investigation of an incident or crime.

6.2 If there are good reasons for retaining CCTV recordings for longer than standard 30-day retention period specified above (such as the investigation of an incident or crime), then this is permitted, if the recordings are deleted as soon as the reason ceases to exist. For example, where a CCTV recording is required for evidential purposes in legal or company disciplinary proceedings, it may be kept until such time as it is no longer needed.

6.3 Once CCTV recordings are no longer needed or the retention period has expired, they should be securely and permanently destroyed or erased.

7 HOW WE PROCESS PERSONAL DATA RECORDED BY CCTV CAMERAS

7.1 It is important that access to, and disclosure of, CCTV recordings is restricted and carefully controlled. This will ensure that the rights of individuals are preserved and ensure that the continuity of evidence remains intact should the recordings be required for evidential purposes e.g. a police enquiry or an investigation being undertaken as part of our disciplinary procedures.

7.2 The following sections of this Procedure explain our rules regarding the viewing of CCTV recordings and their disclosure to third parties.

Viewing images

7.3 Generally, CCTV should only be viewed and accessed by the Information Security Manager and authorised personnel who have been trained in the use of the system. For avoidance of doubt, these are:

a) Information Security Officer;

b) Chief Operations Officer;

c) Hotel Manager;

d) Hotel Manager on Duty;

e) IT technicians;

f) Employees of CCTV service providers; and

g) Director of Legal Affairs.

7.4 Other personnel and third parties (such as the police) should only be allowed to view CCTV footage where it is necessary in connection with the purposes set out in section 4.2 above or as otherwise permitted in this Procedure. Please note permission to view CCTV footage will not be granted to anyone whose role is not explicitly identified in this Procedure. The Director of Legal Affairs will then be responsible for viewing the images to assess if the release of the footage would be in keeping with local data protection and privacy legislation.

7.5 The mere act of viewing is a processing activity that is subject to relevant data protection legislation. As such, the following rules apply to the viewing of CCTV recordings:

a) the viewing of live recordings on monitors is restricted to the authorised personnel listed above whose role requires them to have access to such data; and

b) recorded images should be viewed in a restricted area (e.g. a designated secure office). Access to this area should be restricted whilst the viewing is taking place.

Disclosure of recordings to third parties

7.6 In certain circumstances, it may be necessary to disclose the CCTV recordings to a third party, such as the police. The disclosure is likely to involve the physical delivery of the recordings or copies to the third party (e.g. on a password-protected USB or by email).

7.7 Disclosures to third parties must be consistent with the purposes set out in section 4.2 of this Procedure and in accordance with applicable data protection law.

7.8 Generally, citizenM will not disclose recordings of individuals to third parties unless such individuals have consented to the disclosure or, it is permitted by local data protection legislation to comply with the request without the consent of the relevant individual. It may be appropriate to release images where the needs of the requester outweigh those of the individuals whose images are recorded.

7.9 For example, disclosures may be permitted in the following circumstances:

a) Crime prevention purposes (i.e. preventing or detecting crime, apprehending or prosecuting offenders). The third party making the request must:

- justify its request for the CCTV recording;

- confirm that a failure to make the disclosure would be likely to prejudice any of the crime or taxation purposes;

- put their request in writing, signed by a senior police officer; and

- if required by applicable law, obtain the consent of the relevant data subject(s).

b) Statutory or other legal obligation (i.e. may be required under statute other than data protection legislation, or otherwise be legally required i.e. under a court order). In this situation:

- we must disclose the CCTV recording if the statutory provision imposes upon us a mandatory duty to disclose or a court order requires disclosure; and

- we can choose whether to disclose the CCTV images if the statutory provision imposes upon us a discretion as to whether or not to disclose.

7.10 In limited circumstances it may also be possible to make a disclosure where it is necessary for the purpose of establishing, exercising or defending legal rights, obtaining legal advice or in connection with legal proceedings. This covers not just our legal rights but also those of third parties.

8 THIRD PARTY REQUESTS FOR ACCESS AND/OR DISCLOSURE

8.1 If you receive a request from a third party (such as the police) for the disclosure of CCTV recordings, you must speak to the Director of Legal Affairs in the first instance.

8.2 All third parties who request access to or copies of any CCTV recordings (e.g. police, solicitors) must complete the form set out at Appendix 1 and return it to the Information Security Manager. Law enforcement agencies must also provide proof of legitimacy for their request in writing, with proof of permission to seek the footage. The Director of Legal Affairs will then be responsible for viewing the images to assess if the release of the footage would

be in keeping with local data protection and privacy legislation.

8.3 Urgent requests will be processed as soon as possible i.e. where there is an immediate risk to health and safety or where a crime has been suspected.

8.4 Non-urgent requests will be processed within 10 working days.

Safeguarding

8.5 Requests in relation to a safeguarding incident supersede this Procedure. Requests may be made by any member of staff in an emergency on any property.

8.6 Staff should contact those staff named in section 7.3 of this Procedure and efforts should immediately be made to assist the enquiry.

8.7 Staff who have access to the CCTV systems must comply with requests immediately.

Disclosure

8.8 Where a decision has been made to disclose CCTV recordings, the disclosure must be made securely so that the recordings are received by the intended recipient only.

8.9 For example, where a wireless transmission system is used to disclose the recordings, sufficient safeguards must be put in place to protect the transmission from being intercepted in transit (e.g. encryption or password protection). Alternatively, the CCTV recordings could be viewed in a closed area by the appointed personnel listed in section 7.3 only unless they explicitly give permission for another individual to be there (in relation to the content of the images i.e. to identify an individual).

8.10 All occasions of CCTV footage being viewed, released or otherwise disclosed must be documented via the form in Appendix 1 and forwarded to Information Security.

9 DATA SUBJECT ACCESS REQUESTS

9.1 Under data protection legislation, individuals have a right to access personal data which we process about them, which includes (in some cases) CCTV recordings of them.

9.2 If you receive a request from an individual asking to see CCTV recordings involving him or her or otherwise mentioning access to personal data, you must comply with the citizenM Data Subject Rights Procedure. If the individual does not complete the Data Subject Access Request Form fully, we must at least ask them to provide details of the date and time of the recording they wish to see, the location where the footage was captured, and if necessary information enabling us to identify the individual.

9.3 Upon receipt of the completed Data Subject Access Request Form, the Director Legal Affairs will determine whether disclosure is appropriate and will respond to the individual (with access to the recordings or confirmation of a refusal) within the timescales set down by data protection legislation and in accordance with the citizenM Data Subject Rights Procedure.

9.4 Please note that there are timescales set by data protection legislation within which a request must be handled, therefore you should act quickly and in accordance with the citizenM Data Subject Rights Procedure. For example, in the UK, Switzerland and all EU

member states, you must respond to a data subject access request without undue delay and at the latest within one month from the date of receipt of the request, unless an extension applies. In Taiwan, you must respond to a data subject access request within 15 days from the date of receipt of the request, extendable to another 15 days. In Malaysia, you must respond to a data subject access request within 21 days from the date of receipt of the request, although this period is subject to a further extension of 14 days where the data user has notified the data subject that they are unable to comply with their request within the initial 21 day timeframe.

9.5 If the CCTV recordings of the individual making the request include the images of other identifiable individuals, it may be necessary to obscure or withhold the images of the other individuals if providing their images to the requestor would adversely and disproportionately affect the rights and freedoms of other individuals in the material. Where there is no adverse and/or disproportionate effect on the rights and freedoms of other individuals, then it may not be necessary to obscure the other individuals' identities, unless applicable data protection law requires this.

9.6 If we are able to demonstrate that we are not in a position to identify the individual (for example, where we would likely have to go through a large amount of stored material in order to find the individual in question), we must inform the data subject accordingly, if possible. In such a situation, in our response we should inform the individual about the exact area for CCTV monitoring and confirm which cameras that were in use at the time, so that the individual will have the full understanding of what personal data of him/her may have been processed.

9.7 If a decision is made not to grant the requestor access to some or all of the CCTV recordings (e.g. because there would be an invasion of another person's privacy), we make a record of:

a) the reason for reaching this conclusion;

b) the details of the request (including the date it was made); and

c) the name of the person who made the decision not to provide access. 9.8 In addition to the right of access, data protection legislation also gives individuals various other rights in relation to their personal data (and, as explained above, CCTV recordings of an individual will in most cases be their personal data). These rights include the right to object, the right to erasure and the right to restriction. If you receive a request from an individual seeking to exercise any of these rights, please refer to the citizenM Data Subject Rights Procedure. Again, there are timescales within which a request must be handled, therefore you should act quickly.

10 COMMUNICATION PLAN

Relevant staff will be made aware of this Procedure. Signage will also be displayed on all properties to inform staff, contractors, guests, visitors and the public of the presence of CCTV surveillance, in accordance with this Procedure.

11 REVIEW

11.1 This Procedure will be periodically reviewed (and if necessary updated) annually for the continued justification for and effectiveness of our CCTV system, or sooner if required to reflect changes in data protection legislation or circumstance. We will also audit compliance with this Procedure.

11.2 On request, you will provide the Information Security Officer with all reasonable assistance in the performance of these periodic reviews and audits and take all necessary steps to implement any recommendations or changes which result from such reviews.

11.3 If a material change to our use of CCTV (to the technology involved, to the purposes for which CCTV is used etc.) is proposed, we will carry out a data protection impact assessment prior to making any changes.

12 CHANGES TO THIS PROCEDURE

12.1 We reserve the right to change this Procedure from time to time to consider any relevant changes in data protection legislation and/or relevant guidance. Changes to this Procedure will be communicated to all relevant staff.

Third Party Request to view CCTV recordings

This form is required to be filled in each time a request is made by a third party (such as the police) to view any data from any citizenM CCTV camera, in compliance with relevant data protection law.

Date:

.....

Name of Requester:

.....

Preferred telephone number:

.....

Your current home or work address (to which we will reply):

.....

.....

Date of CCTV recording to be viewed

From: **To:**

.....

Time of CCTV recording to be viewed

From: **To:**

.....

Details of CCTV recording (including camera location(s), if known) and reasons for the request:

.....

.....

.....

.....

.....

.....

Details of any identifying features to help establish your identity or the identity of the individual of whom you request the data:

.....

.....

.....

.....

.....

Declaration (to be signed by the applicant)

The information that I have supplied in this application is correct and I am either a) the person to whom it relates, or b) a relevant third party who has attached proof of legitimacy for my request in writing, with proof of permission to seek the footage, to this form.

Signed by:

.....

Date:

.....

Information Security Officer's signature:

.....

Date:

.....

Director Legal Affairs Authorisation:

.....

Date:

.....

Request Denied:

.....

Date:

.....

Reason for denied request:

.....

.....

.....

.....

.....

.....

.....

Review carried out by:

.....

Date:

.....

Time:

.....

Conclusions of review:

Additional action required:

Escalated to:

Date: