Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-023[1]

13 June 2019

[redacted]

Re: PROCESSING OF CCTV FOOTAGE UNDER THE DATA PRIVACY ACT OF 2012

Dear [redacted],

We write in response to your request for advisory opinion received by the National Privacy Commission (NPC) which sought to clarify the following matters regarding Data Privacy Act of 2012[2] (DPA):

1. Whether the use of the closed-circuit television (CCTV) is allowed under the DPA; and
2. Whether the CCTV footage is admissible as evidence in court.

Scope of the DPA; CCTV footage as personal information; lawful processing of personal information

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in the processing of personal information.

Personal information is any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[3]

[1] Tags: scope, lawful processing of personal information, privacy notice, CCTV, employee, evidence
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[3] Data Privacy Act of 2012, § 3 (g)

A CCTV is a camera surveillance system that captures images of individuals or information relating to individuals.[4] Accordingly, if a camera surveillance footage is of sufficient quality, a person with the necessary knowledge will be able to reasonably ascertain the identity of an individual from the footage.[5]

As can be gleaned from the foregoing, the footage and images captured in the CCTV, as a general rule, are considered personal information, and the provisions of the DPA, specifically Section 12, will apply:

a. The data subject has given his or her consent;
b. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
c. The processing is necessary for compliance with a legal obligation to which the personal information controller (PIC) is subject;
d. The processing is necessary to protect vitally important interests of the data subject, including life and health;
e. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
f. The processing is necessary for the purposes of the legitimate interests pursued by the PIC or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

Concomitant to the above, the processing of CCTV footage is allowed under the DPA if the same is necessary under any of the abovementioned criteria, subject to the implementation of a reasonable and appropriate organizational, physical and technical security measures and adherence to the general data privacy principles of transparency, legitimate purpose and proportionality.

In addition, Section 13(f) of the DPA may likewise apply where a CCTV footage or image would reveal sensitive personal information. Thus, the processing of CCTV footage may be allowed if the same is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

Processing of personal information in the workplace;
Legitimate interest of employer

You mentioned in your letter that your client, as the employer, installed CCTV and surveillance cameras in the workplace. Footages then revealed irregularities and fraudulent activities carried out that resulted to the modification of the accounts of postpaid subscribers. Your client then intends to use the video footages as evidence in filing criminal charges against its employees.

[4] See: Office of the Privacy Commissioner (New Zealand). Privacy and CCTV: A guide to the Privacy Act for businesses, agencies and organizations (2009), *available at* https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf (last accessed Oct. 16, 2018).
[5]See: Office of the Information Commissioner (Queensland). Camera Surveillance and Privacy (2009), *available at* https://www.oic.qld.gov.au/__data/assets/pdf_file/0010/28099/guideline-camera-surveillance-and privacy.pdf (last accessed March 21, 2019).

Every employer may have a legitimate interest in processing personal information of its employees through the CCTV, particularly in keeping employees safe, preventing crime and detecting employees' misconduct.

Legitimate interest refers to matters that are desired by or important to a PIC, which must not be contrary to law, morals or public policy. This includes business, financial or other reasonable purpose.

In order to use legitimate interest as basis for lawful processing, a PIC must consider the following:

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
2. Necessity test - The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PICs or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects should not be overridden by the legitimate interests of the PIC, considering the likely impact of the processing on the data subjects.[6]

Employee monitoring; right to be informed; privacy notice in the workplace

The DPA imposed obligations on PICs to uphold the rights of the data subject to be informed and notified[7] in the processing operations performed on their personal data. Specifically, every PIC is required to craft and implement policies and procedures regarding the collection, use, access, storage and destruction of footages. The exact purpose of processing and extent of such activities should likewise be indicated.

Employees must likewise be properly informed and oriented about the policy on CCTV and surveillance cameras, including the place, time, and circumstances of such recording. There must be a privacy notice on conspicuous areas to apprise the data subjects, employees in this case, that the premises or particular areas are under surveillance.

Likewise, we wish to emphasize that although employees are within office premises and using company-issued equipment within office hours, they still are entitled to their right to privacy at work.[8] With the emergence of new technologies that provide employers with vast opportunities to monitor and track employees, unbridled checking can damage trust, disrupt professional relationships and disturb workplace peace and performance.[9]

---

[6] See: National Privacy Commission, NPC Advisory Opinion No. 2018-061 (Sept. 6, 2018) citing Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/ [last accessed on September 5, 2018].

[7] Data Privacy Act of 2012, § 16 (a) and (b).

[8] National Privacy Commission, NPC Advisory Opinion No. 2018-084 (Dec. 4, 2018).

[9] *Id.* citing Privacy Commissioner of New Zealand- Privacy at Work: A guide to the Privacy Act for employers and employees, accessed on 28 November 2018, available at https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-at-Work-2008.pdf

Admissibility of CCTV footage as evidence in court

We understand that Rule 11, Section 1 of the Rules on Electronic Evidence provides that audio, photographic and video evidence of events, acts or transactions shall be admissible provided it shall be shown, presented or displayed to the court and shall be identified, explained or authenticated by the person who made the recording or by some other person competent to testify on the accuracy thereof.[10] To be admissible, evidence must be competent and relevant. The former requires that the evidence is not excluded by the law or by the Rules of Court while the latter provides that the evidence has a relation to the fact in issue as to induce belief in its existence or non-existence.

Please note however, that the determination of the admissibility of evidence in court is not within the purview of NPC's mandate. This matter is governed by the Rules of Court and other applicable rules of the Supreme Court, such as the Rules on Electronic Evidence.

This opinion is based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of facts.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[10] Supreme Court, Rules on Electronic Evidence, A.M. No. 01-7-01-SC, (July 17, 2001).