Quisumbing Torres.
Member Firm of Baker & McKenzie International

Client Alert
24 August 2024

Philippines: Updated framework issued on the use of closed-circuit television systems

The National Privacy Commission recently issued Circular No. 2024-02, which provides an updated policy framework on the use of closed-circuit television systems.

In brief

The National Privacy Commission (NPC) recently issued NPC Circular No. 2024-02 ("**Circular**"), which provides an updated policy framework on the use of closed-circuit television (CCTV) systems. The Circular is intended to address emerging privacy risks arising from the use of CCTV systems, and to enable data controllers and processors to properly manage personal data processing carried out through such systems.

In this issue

In more detail
Recommended actions

The more comprehensive Circular modifies the previously issued NPC Advisory No. 2020-04, which was the guidance on the use of CCTV systems since November 2020. The Circular takes effect on **27 August 2024**.

Clients are advised to review their policies and notices on the use of CCTV systems to ensure that these are aligned with the newly issued framework.

In more detail

Personal information controllers (PICs) and personal information processors (PIPs) must ensure that the use of CCTV systems adheres to the general principles of privacy and upholds data subjects' rights and freedoms. PICs and PIPs must adhere to the principles of transparency, legitimate purpose, proportionality and data minimization, and accountability when using CCTV systems. Any processing must also be carried out pursuant to an appropriate lawful basis under the Data Privacy Act (DPA), and there must be safeguards in place for the protection of personal data. Moreover, PICs and PIPs shall establish policies allowing data subjects access to their personal data that is recorded on CCTV systems.

Applicability of the Circular

The Circular applies to all PICs and PIPs engaged in the processing of personal data through CCTV systems, except for the following:

1. CCTV systems that are used for personal, family or household affairs, or when used for lawful surveillance.[1] A CCTV system is considered to be used for personal, family or household affairs when use is limited to those with no connection to any professional activity and not intended for profit or commercial gain. This includes the use of CCTV for home security purposes within the premises and boundaries of a private and noncommercial residence or establishment. Nevertheless, the totality of the circumstances surrounding the processing will be considered in determining whether the specific processing activity falls under this exception.

   In determining whether a specific processing activity falls outside the scope of the personal, family or household affairs exception, the following factors must be considered:

   a. Dissemination of personal data to an indefinite number of people

[1] Circular, Sec. 1.

b. Processing that may have an adverse impact on the rights and freedoms of the involved data subjects

c. Processing of personal data about data subjects who have no personal, family or household relationship with the person engaged in the processing

Further, this exception does not apply where CCTV systems capture images of individuals beyond the boundaries of a private and noncommercial residence or establishment, particularly where it monitors a public space. In such cases, the owner of the CCTV systems is a PIC and subject to the corresponding obligations under the DPA, its Implementing Rules and Regulations, and all relevant issuances of the NPC.[2]

2. Law enforcement, intelligence and investigative agencies, and other government agencies conducting lawful surveillance in accordance with their respective mandates. Nonetheless, these agencies shall be subject to the applicable requirements of the Philippine Constitution and other laws and regulations regulating surveillance activities.

General principles of data processing as applied to CCTV systems

PICs and PIPs must adhere to the principles of transparency, legitimate purpose, proportionality and data minimization, and accountability when using CCTV systems.

The principle of transparency requires that information about the use of CCTV systems be made available to the data subjects in the most appropriate format and in clear, plain and concise language. CCTV notices must be readily visible and prominently displayed in conspicuous areas, such as points of entry. Data subjects must also be informed about the nature, scope and extent of surveillance, purpose, capabilities of the CCTV systems, among other necessary information.[3] Moreover, in line with the principle of legitimate purpose, PICs shall ensure that the purpose of processing is not contrary to law, morals or public policy, and that such purpose is clearly determined, specified and declared to the data subject prior to the use of the CCTV systems.[4]

PICs and PIPs are also required to adhere to the principle of proportionality and data minimization. PICs shall ensure that the use of CCTV systems remains necessary and proportional to the specified and declared legitimate purpose. PICs and their PIPs shall regularly review their use of CCTV systems to determine if the purpose of the processing could not reasonably be fulfilled by any other less intrusive means, and to ensure that the personal data processed is limited to that which is adequate, relevant, suitable, necessary and not excessive in relation to such purpose.[5]

CCTV systems must also be operated in a fair and lawful manner. The processing of personal data using CCTV systems shall be neither manipulative, oppressive nor discriminatory.[6] Further, in accordance with the principle of accountability, PICs shall be responsible for personal data processed using CCTV systems and shall use contractual or other reasonable means to ensure proper safeguards are in place when the processing is subcontracted to PIPs.[7]

Lawful basis and safeguards for processing

The Circular obliges PICs to determine the more appropriate lawful basis other than the consent of the data subject for the processing of their personal data through the use of CCTV systems. PICs must take into account that the purpose of using CCTV systems will vary and consent may not be the most suitable lawful basis in the context of specific processing activities, such as those involving open surveillance in public and semipublic places.[8]

---

[2] Circular, Sec. 1.

[3] Circular, Sec. 3(A).

[4] Circular, Sec. 3(B).

[5] Circular, Sec. 3(C).

[6] Circular, Sec. 3(D).

[7] Circular, Sec. 3(E).

[8] Circular, Sec. 4.

In addition, PICs and their PIPs must implement reasonable and appropriate security measures, including privacy-by-design principles, to protect personal data processed against accidental, unlawful or unauthorized use, to minimize privacy intrusion and to comply with the requirements under privacy regulations.[9]

PICs and PIPs must implement reasonable and appropriate safeguards to ensure and maintain the integrity and accuracy of the footage recorded and stored, including any associated metadata (e.g., time, date and location) that may facilitate access requests for CCTV footage.[10] Footage recorded by CCTV systems shall be stored in a secure and encrypted manner to ensure its confidentiality, integrity and availability.[11] As for retention of data, the Circular clarified that while there is no specific retention period for CCTV footage, such footage shall be retained only for as long as necessary to fulfill the purpose for which the CCTV footage was obtained.[12]

In addition, PICs and PIPs are required to establish policies that govern the operation of CCTV systems. These policies should include information on the operational details of CCTV systems, the designation of authorized personnel who are responsible for handling access requests and the day-to-day operation of the CCTV systems, and a documented retention policy containing the retention period of CCTV footage and the manner of disposal or destruction when the retention period has lapsed, among others.[13]

Moreover, PICs and PIPs must thoroughly consider the location and angles of cameras, and ensure that CCTV systems capture footage in a manner that avoids unreasonable intrusions on the data subjects' privacy. The advanced functionalities of CCTV systems, such as zoom and rotation capabilities, must not be used in the surveillance of private spaces.[14]

Right to access; third-party access

The Circular also lays down a framework to allow data subjects to access their data that is recorded on CCTV systems, and requires PICs and PIPs to establish policies allowing for access. Requests for access may include both viewing and obtaining a copy of CCTV footage.[15]

PICs and PIPs are required to act upon requests for access without undue delay. The period to respond shall not exceed five working days from receipt of the request when the request is for viewing only. On the other hand, the period shall not exceed 15 working days from the receipt of the request when the request involves obtaining a copy of the CCTV footage.[16]

PICs and PIPs may require the presentation of supporting documentation when evaluating requests for access. For persons requesting access for and on behalf of another, PICs and PIPs may request evidence of proper authorization and other supporting documents to validate the authority and identity of the representative, as well as to confirm the identity of the requesting party. Data subjects must also provide sufficient details on the requested footage, such as the specific date, approximate time and location, to enable PICs and their PIPs to locate such footage.[17]

The Circular also establishes a framework for third-party access to CCTV footage. CCTV footage may be disclosed in cooperation with criminal investigations conducted by law enforcement agencies, as well as in compliance with a lawful order of a court of competent authority. CCTV footage may also be disclosed for the purposes of an administrative investigation,

---

[9] Circular, Sec. 5.

[10] Circular, Sec. 5(B)(2).

[11] Circular, Sec. 5(B)(3).

[12] Circular, Sec. 5(B)(4).

[13] Circular, Sec. 5(A).

[14] Circular, Sec. 5(B)(1).

[15] Circular, Sec. 6(A).

[16] Circular, Sec. 9(A).

[17] Circular, Sec. 6(A).

provided that there is sufficient proof of the investigation being conducted or the pending complaint before an administrative body.[18]

As for requests from the media, the Circular clarified that PICs and PIPs are not obliged to release CCTV footage to the media, unless there is a lawful basis for processing under sections 12 or 13 of the DPA, or processing under a special case, specifically Section 4 (d) of the DPA. Further, the disclosure should always be with due regard to the general principles of privacy, rights of data subjects, and codes of conduct and ethical standards of journalism. PICs and PIPs are prohibited from disclosing CCTV footage of identifiable individuals to the media for amusement or entertainment purposes, unless it is with the consent of the data subject. Where the media's request involves images of individuals other than the specific person sought to be identified for news reporting, the requesting media personnel or journalist must mask the images of those other individuals before making the footage public.[19]

Any other third-party access requests for CCTV footage and images shall be evaluated with greater scrutiny to prevent violation of the privacy rights of the data subjects concerned.[20]

Requests for access to CCTV footage may be denied upon appropriate evaluation.[21] PICs can only deny a request after giving the data subject or third party a reasonable opportunity to amend the request. Should the PIC deny a request for CCTV access, it shall provide the requesting party with the reason for the denial within five working days from receipt of the request.[22]

The following reasons are appropriate grounds for denial of a request:[23]

1. The data subject provided incomplete information regarding the requested CCTV footage. The person making the request must first be given a reasonable opportunity to amend the request and to provide complete information.
2. The access request is frivolous or vexatious.
3. The purpose for and manner of viewing or obtaining a copy of the footage is contrary to law, morals or public policy.
4. The request to obtain a copy of the CCTV footage is disproportional to the purpose stated by the requesting party.
5. The burden or expense of providing access would be unreasonable or involve disproportionate effort on the part of the PIC or PIP.
6. The footage has already been deleted by the time the PIC or its PIP received the request pursuant to its documented retention policy.
7. Disclosure of the footage could put an ongoing criminal investigation at risk, as determined by the appropriate public authority. For this purpose, the PIC should provide written proof of this determination.

Effectivity

The Circular takes effect on 27 August 2024. PICs and PIPs are given a period of 60 calendar days from the effectivity of the Circular, or until 26 October 2024, to comply with its requirements.

---

[18] Circular, Sec. 7(B), pars. 1-3.

[19] Circular, Sec. 7(B), par. 4.

[20] Circular, Sec. 7(B), par. 5.

[21] Circular, Sec. 10.

[22] Circular, Sec. 10(B).

[23] Circular, Sec. 10(A).

Recommended actions

Clients are advised to review their use of CCTV systems to ensure that these systems are in compliance with the Circular. Clients should ensure that the appropriate CCTV notices are posted in their premises, and must likewise ensure that there are appropriate policies in place governing the use and operation of these CCTV systems.

Clients must review existing internal mechanisms to ensure that there is a framework for allowing data subjects access to their CCTV footage, as provided for in the Circular.

Clients are likewise encouraged to stay tuned for further updates from the NPC on its implementation of the Circular.

Contact Us

Bienvenido A. Marquez III
Partner
Intellectual Property, Data and Technology
Quisumbing Torres, Manila
bienvenido.marquez
@quisumbingtorres.com

Divina P.V. Ilas-Panganiban, CIPM
Partner and Head
Intellectual Property, Data and Technology
Quisumbing Torres, Manila
divina.ilas-panganiban
@quisumbingtorres.com

Marianne Angeli B. Estioco
Associate
Intellectual Property, Data and Technology
Quisumbing Torres, Manila
marianneangeli.estioco
@quisumbingtorres.com

Follow us on LinkedIn! | Visit our Website