NPC Circular No. 2024 – 02

DATE : 9 August 2024

SUBJECT : CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS

WHEREAS, the National Privacy Commission (NPC) previously issued NPC Advisory No. 2020-04, or the Guidelines on the Use of Closed-Circuit Television (CCTV) Systems, which provides guidance to all personal information controllers (PICs) and personal information processors (PIPs) on the use of CCTV systems operating in public and semi-public areas;

WHEREAS, CCTV systems process personal and sensitive personal information (collectively, personal data);

WHEREAS, there is a need to provide an updated policy framework on the use of CCTV systems as the technology for such systems is continuously evolving, and the use of the same has become accepted and even mandated in certain instances;

WHEREAS, these guidelines are necessary to address emerging privacy risks, and enable PICs and PIPs to properly manage personal data processing through CCTV systems;

WHEREAS, PICs and PIPs must ensure that the use of CCTV systems adheres to the general principles of privacy and upholds data subjects' rights and freedoms;

WHEREFORE, in consideration of the foregoing premises, the NPC hereby issues this Circular on CCTV systems.

SECTION 1. ***Scope.*** **—** This Circular shall apply to all PICs and PIPs engaged in the processing of personal data through CCTV systems, except when CCTV systems are used for any of the following purposes:

A. *Personal, family, or household affairs.* This Circular shall not apply to the use of CCTV systems for purely personal, family, or household affairs as defined herein.

   Where CCTV systems capture images of individuals beyond the boundaries of a private and non-commercial residence or establishment, particularly where it monitors a public space, such use cannot be considered purely for personal, family, or household use. As such, the owner of the CCTV systems is a PIC and subject to the corresponding obligations under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and all relevant issuances of the NPC.

B. *Lawful surveillance*. This Circular shall not apply to law enforcement, intelligence, and investigative agencies and other government agencies conducting lawful surveillance

in accordance with their respective mandates. Nonetheless, they shall be subject to the applicable requirements of the Philippine Constitution and other laws and regulations regulating surveillance activities.

SECTION 2. ***Definition of Terms.*** **—** The definition of terms used in the DPA and its IRR, as amended, and other NPC issuances are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. "Commission" refers to the Privacy Commissioner and the two (2) Deputy Privacy Commissioners, acting as a collegial body;

B. "Closed-Circuit Television" or "CCTV" refers to closed-circuit television or camera surveillance systems in a fixed or stationary location that can capture images of individuals or other information relating to individuals;

C. "Masking" refers to the process of obscuring or hiding parts of a video or image from being viewed, like blurring or covering faces, body parts, or other objects that will reveal personal data;

D. "NPC" refers to the National Privacy Commission created under the DPA;

E. "Personal, family, or household affairs" refers to the uses that are limited to those with no connection to any professional activity and not intended for profit or commercial gain. For purposes of this Circular, this includes the use of CCTV for home security purposes within the premises and boundaries of a private and non-commercial residence or establishment. Nevertheless, the totality of the circumstances surrounding the processing will be considered in determining whether the specific processing activity falls under the exception in Section 1 (A) of this Circular.

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

   1. Dissemination of personal data to an indefinite number of people;
   2. Processing may have an adverse impact on the rights and freedoms of the involved data subjects; or
   3. Processing of personal data about data subjects who have no personal, family, or household relationship with the person engaged in the processing.[1]

F. "Public authority" refers to any government entity created by the Philippine Constitution or law;

G. "Public space" refers to streets and alleys, public parks, schools, buildings, malls, bars, restaurants, transportation terminals, public markets, spaces used as evacuation centers, government offices, public utility vehicles as well as private vehicles covered

[1] See: National Privacy Commission, KEC v. JMP [NPC 19-764] (November 11, 2021) and ARTICLE 29 DATA PROTECTION WORKING PARTY Statement of the Working Party on current discussions regarding the data protection reform package, Annex 2 Proposals for Amendments regarding exemption for personal or household activities (2013).

by app-based transport network services and other recreational spaces such as, but not limited to, cinema halls, theaters and spas;[2]

H. "Semi-public space" refers to any indoor or outdoor space that, even if privately owned, is open or accessible to the public during its operating hours;

I. "Video analytics" refers to any technology that processes a digital video signal using a special algorithm to perform a security-related function. The common types of video analytics are fixed algorithm analytics, artificial intelligence learning algorithms, and facial recognition systems.[3]

SECTION 3. ***General principles.*** **—** PICs and its PIPs engaged in the processing of personal data through CCTV systems are mandated to ensure that reasonable and appropriate safeguards are in place for the protection of personal data, taking into account the rights of the data subject. For this purpose, PICs and its PIPs shall adhere to the following principles:

A. *Transparency*. PICs shall provide appropriate CCTV notices to inform data subjects of the existence and purpose of CCTV systems in operation. Given that CCTV notices are a specific kind of privacy notice, the requirements for privacy notices as stated in NPC Circular No. 2023-04 or the Guidelines on Consent shall apply. In addition, PICs shall ensure that CCTV notices adhere to the following:

1. Information about the use of CCTV systems shall be made available to the data subjects in the most appropriate format and in clear, plain, and concise language.
2. These CCTV notices shall be readily visible and prominently displayed within the appropriate premises, such as but not limited to, points of entry or other conspicuous areas.
3. The nature, scope, and extent of surveillance, purpose, capabilities of the CCTV systems, and other necessary information shall be provided to the data subjects in accordance with their right to be informed under the DPA.

B. *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]

C. *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 its PIPs shall regularly review its use of CCTV systems to determine if the purpose of the processing could not reasonably be fulfilled by any other less intrusive means, and if the personal data processed is limited to that which is adequate, relevant, suitable, necessary, and not excessive in relation to the purpose.

D. *Fairness and Lawfulness*. The processing of personal data using CCTV systems shall be neither manipulative, oppressive, nor discriminatory. PICs shall ensure that the means

[2] An Act Defining Gender-Based Sexual Harassment in Streets, Public Spaces, Online, Workplaces, and Educational or Training Institutions, Providing Protective Measures and Prescribing Penalties Therefor [Safe Spaces Act] (2019) Republic Act No. 11313 (2019).
[3] See: Science Direct, Video Analytics, citing Electronics Elements, Thomas L. Norman CPP, PSP, CSC, in Effective Physical Security (Fifth Edition), 2017, available at https://www.sciencedirect.com/topics/computer-science/video-analytics (last accessed 31 March 2023).
[4] National Privacy Commission, MLF v. MYTAXI.PH CORPORATION (GRAB PHILIPPINES) [NPC 19-142] (March 21, 2022).

and method of the processing shall be in accordance with law, morals, public policy, and good customs.

E. *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. PICs shall demonstrate compliance by adhering to the general principles of privacy, implementing safeguards, keeping appropriate records, upholding data subject rights and their other obligations under the DPA, IRR, and relevant issuances of the NPC.

SECTION 4. ***Lawful basis.*** **—** PICs shall identify the most appropriate lawful basis for processing under the DPA and the same should be provided when required by the Commission.

A. PICs shall 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 consider 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 semi-public places.

B. The processing of CCTV footage including sensitive personal information shall be based on the most appropriate lawful basis under Section 13 of the DPA.

SECTION 5. ***Safeguards.*** **—** PICs and its PIPs shall implement reasonable and appropriate security measures, including privacy by design principles, to protect personal data processed against accidental, unlawful, or unauthorized use,[5] to minimize privacy intrusion, and to comply with the requirements under the DPA, its IRR, and relevant issuances of the NPC.

A. *Policies*. PICs and its PIPs shall establish policies that govern the operation of CCTV systems, which include:

1. Information on the legitimate purpose;
2. Information on the lawful basis for processing;
3. Regular conduct of privacy impact assessments (PIAs) and regular review of the use of the CCTV systems;
4. CCTV notice and placement thereof;
5. Operational details of the CCTV systems, such as but not limited to, procurement, installation, operation, control, monitoring, maintenance, incident response and reporting;
6. Designation of authorized personnel who shall be responsible for handling access requests, monitoring live feeds, and the day-to-day operation of the CCTV systems;
7. Subject to Sections 6 to 8 of this Circular, the policy shall provide procedures for the following:
   a. Requests for access to CCTV footages, whether for viewing or providing a recording or copy thereof;
   b. Handling inquiries and complaints, if any; and

[5] Data Privacy Act of 2012, § 20 (2012).

c. Managing personal data breaches and security incidents involving the CCTV systems;

8. Documented retention policy containing the retention period of CCTV footage and manner of disposal or destruction when the retention period has lapsed. The documented retention policy shall be included in the CCTV policy;
9. Security measures to be implemented for the protection of CCTV footage against any accidental, unauthorized, or unlawful processing, including access (e.g. copying or viewing), alteration, destruction, or disclosure, and the conduct of regular evaluation and audit of such security measures; and
10. Process for the regular review and assessment of the policy document, audits to determine if the policy is being implemented and complied with, and policy revision and updates.

B. *Deployment and operation*. PICs and its PIPs shall be subject to the following parameters upon the implementation of CCTV systems:

1. *Location and placement*. To ensure that CCTV systems capture footage in a manner consistent with the DPA and to avoid unreasonable intrusions on the data subjects' privacy, the PIC and its PIPs shall thoroughly consider the location and angles of the cameras.
   a. CCTVs shall only be used to monitor the intended spaces, taking into consideration the purpose for such monitoring;
   b. Should the CCTV systems have zoom and rotation capabilities, PICs and PIPs shall ensure that such functionalities will not result in surveillance of private spaces (*e.g.*, private backyards, through windows of private residences); and
   c. Use of CCTVs in areas where individuals have a heightened expectation of privacy (*e.g.*, fitting rooms, rest rooms, toilets, lactation or breastfeeding rooms,) is strictly prohibited.

2. *Quality and integrity of data*. To sufficiently fulfill the intended purposes for installation, PICs shall ensure that the data captured and recorded by CCTV systems be of appropriate and suitable quality. PICs and its PIPs shall 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.

3. *Storage*. Footage recorded by CCTV systems shall be stored in a secure manner, whereby its confidentiality, integrity, and availability are ensured. The recorded footage shall be encrypted pursuant to the applicable issuances of the NPC.
   a. Without prejudice to the exercise of the right to access of data subjects and third-party access requests, access to the area where the CCTV footage is stored shall be restricted to authorized personnel only;
   b. Access logs for the CCTV footage, including access requests, reproductions, and transfers, shall be updated on a regular basis as determined by the PIC; and
   c. PICs and PIPs shall restrict monitoring of live CCTV feeds to authorized personnel only. It shall identify and state in its CCTV policy the personnel authorized to monitor such live feeds.

4. *Retention.* While there is no specific retention period for CCTV footage, CCTV footage shall be retained only for as long as necessary to fulfill the purpose for which the CCTV footage was obtained.
    a. Retention periods shall not be determined based solely on the storage capacity of CCTV systems.
    b. The retention period shall be clearly documented and form part of the CCTV policy.
    c. CCTV footage shall be destroyed once it is no longer needed for its declared and specified purpose.

5. *Video analytics.* The same requirements shall apply when processing personal data derived from CCTV systems that utilize video analytics. PICs shall utilize PIAs to assess and minimize potential privacy risks.

6. *Assistance of PIPs.* In accordance with Sections 43 and 44 of the IRR, PICs should put in place contractual or other reasonable means to ensure the cooperation and assistance of PIPs they have engaged to process personal data on their behalf.

SECTION 6. ***Data subject request for access.*** **—** Any person whose personal data is recorded on CCTV systems has a right to reasonable access to the same pursuant to Section 16 of the DPA and Section 34 of the IRR.

A. PICs and PIPs shall establish policies allowing for access, and shall consider the following:

    1. Use of a simple and accessible process for submitting requests for access, which includes viewing and obtaining a copy of CCTV footage;
    2. Verification of the identity of the data subject requesting for access through the presentation of supporting documentation, such as IDs or other similar documents: *provided*, that the information required shall only be to the extent necessary to confirm such identity;
    3. For persons requesting access for and on behalf of another, PICs and its 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;
    4. Purpose and manner of the request for access, which should not be contrary to law, morals, or public policy; and
    5. Sufficient details on the requested footage such as the specific date, approximate time, and location, to enable PICs and its PIPs to locate such footage.

B. Where images of persons other than the requesting data subject appear on the CCTV footage, such as a specific person sought to be identified as part of the request for identification of malefactors for the protection of lawful rights and interests, establishing legal claims, investigation, or law enforcement purposes, Section 12 (f) or 13 (f) of the DPA may apply as the basis for the disclosure.

SECTION 7. ***Third-party access request***. **—** A third-party access request is a request to access CCTV footage made by a person other than the data subject involved in the footage or the latter's authorized representative. If a data subject involved in the footage or their authorized representative requests access to CCTV footage, the presence of another person's

image within the CCTV footage does not automatically classify such request as a third-party access request. Further, in handling third-party access requests, the same policies and procedures outlined in the previous section shall apply.

A. PICs shall decide on the merits of the request for disclosure based on the DPA, IRR, relevant issuances of the NPC, and other existing laws and regulations.

    1. Once a PIC has disclosed information to the requesting party, the latter becomes responsible for the copy they hold. It is the requesting party's responsibility to comply with the DPA, its IRR, and other related issuances of the NPC in relation to any processing of the personal data involved in the CCTV footage requested.
    2. The method for disclosing the requested information should be secure to ensure access only by the intended recipient.

B. Subject to the criteria provided for the lawful processing of personal data under Sections 12 and 13 of the DPA, CCTV footage may be disclosed in the following instances:

    1. *Law enforcement and criminal investigations.* With respect to requests for CCTV footage to be disclosed in relation to a criminal investigation, PICs and its PIPs shall cooperate on the appropriate disclosure of CCTV footage to the authorized law enforcement agencies in connection with the latter's constitutional or statutory functions (*e.g.*, criminal investigations, case build-up).
        a. Law enforcement officers shall provide the PIC to whom the request is made with a written statement, affirmative declaration, or equivalent to establish the lawfulness of the request.
        b. The request for CCTV footage shall be made following, and with strict adherence to, existing standard operating procedures in the conduct of an investigation and law enforcement operation as stated in the applicable rules and regulations of law enforcement agencies and other pertinent public authorities.

    2. *Court Order.* Requests for disclosure and use of CCTV footage and images by virtue of a lawful order of a court of competent authority are allowed, taking into consideration the rules on the issuance of subpoenas.

    3. *Administrative investigations.* The use of CCTV footage for purposes of an administrative investigation shall be allowed. The requesting party shall provide sufficient proof of the investigation being conducted or the pending complaint before an administrative body.

    4. *Request from the media.* PICs and its PIPs are not obliged to release CCTV footages 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.
        a. PICs and its PIPs are likewise proscribed from disclosing CCTV footages of identifiable individuals to the media for amusement or entertainment purposes, unless it is with the consent of the data subjects. It is incumbent upon

the media to prove that the requested CCTV footage shall not be used for amusement or entertainment purposes.

b. Law enforcement agencies may release CCTV footage to the media on a case-to-case basis taking into account the lawful basis for processing of personal data under Sections 12 and 13 of the DPA, or processing under a special case, considering the requirements of public order and safety, verification or confirmation of identity, and other relevant factors.
c. 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.

5. *Other third-party requests.* 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.
   a. Upon determination of PICs that the requesting third party's needs outweigh those of the data subjects to whom the CCTV footage and images pertain, it may release information to such requesting third party.
   b. PICs must determine on a case-to-case basis if they will accede to such request taking into consideration the general principles of privacy, the rights and freedoms of the data subjects whose images are recorded by the CCTV systems, and a lawful basis for processing under Section 12 or Section 13 of the DPA.

SECTION 8. ***Response procedure.*** **—** The following shall be implemented:

A. When the requesting party informs the PIC in writing of its intention to view or obtain a copy of a particular CCTV footage, the PIC and its PIPs shall preserve the pertinent CCTV footage by taking the same out of the coverage of the established retention period as indicated in the documented retention policy until such time as any of the following occur:

   1. The access request is fulfilled;
   2. The access request is abandoned by the requesting party; or
   3. In cases where the requesting party files a complaint questioning the PIC's denial of the access request or the NPC conducts an investigation on the matter, and the Commission affirms the PIC's denial of the request.

   A request is deemed abandoned when the requesting party has not fulfilled the requirements in Section 6 or 7 of this Circular, as the case may be, within thirty (30) days from initially informing the PIC of the intention to either view or obtain a copy of the CCTV footage.

B. Upon fulfillment of the requirements in Sections 6 or 7 of this Circular, PICs and its PIPs shall allow access to the CCTV footage through viewing or providing a copy to the data subject or the third party, as the case may be, taking into consideration the stated purpose for the request.

   1. *Viewing.* The requesting party may be allowed a reasonable opportunity to view the requested footage, subject to the following conditions:
      a. CCTV footage shall be viewed in an authorized and secure area;

b. Only the requesting party and the authorized personnel of PICs and their PIPs shall be allowed to view such footage; and
c. Other security measures to ensure confidentiality of the footage to be viewed shall be implemented, such as signing of non-disclosure agreements or prohibiting the capture of the footage through mobile phones and other devices, where appropriate.

2. *Obtaining a copy of the CCTV footage.* The requesting party may be given copies of the CCTV footage subject to the following conditions:
   a. PICs and their PIPs shall ensure that the copying of footage is made in a secure manner that maintains the integrity of the footage and any associated metadata.
   b. In circumstances where there is technical difficulty in providing a copy of the footage in video format, PICs and their PIPs may provide still images as an alternative. Where still images are provided, it would be necessary to supply sufficient stills for the duration of the requested footage.
   c. PICs or their PIPs may charge the data subject or third party a reasonable fee to cover administrative costs for providing a copy of the footage. For this purpose, PICs or their PIPs shall not impose excessive fees in order to discourage such requests.

SECTION 9. ***Period for complying with the request.*** **—** Requests shall be acted upon without undue delay.

A. The period shall not exceed five (5) working days from receipt of the request when the request is for viewing only. The period shall not exceed fifteen (15) working days from the receipt of the request when the request involves obtaining a copy of the CCTV footage.

   The request is considered submitted at the time the requesting party complies with the requirements stated in Section 6 or 7 of this Circular, as the case may be.

B. If a request is complex or involves numerous footage, whether for viewing or obtaining a copy of the CCTV footage, the period to comply with such request may be extended for an additional period not exceeding fifteen (15) working days.

C. In case of an extension, PICs or its PIPs shall notify the data subject or the authorized representative in writing of the intended date of compliance and the reason for the extension.

SECTION 10. ***Denial of request.*** **—** Requests for access to CCTV footage may be denied upon appropriate evaluation.

A. The following are grounds for denial:

   1. Incomplete information regarding the requested CCTV footage, as stated in Section 6: *provided,* that the data subject, their authorized representative, or third party is first given a reasonable opportunity to amend the request and provide complete information;

2. The access request is frivolous or vexatious. The determination of what constitutes frivolous or vexatious may be made on the basis of the particular circumstances of the request;
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 its 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 as stated in Section 5(A)(8) of this Circular; or
7. If 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.

B. 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 (5) working days from receipt of the request: *provided*, that the denial shall not serve as a bar for future requests by the same data subject or third party which complies with Section 6(A)(5) of this Circular on the sufficiency of details on the requested footage.

   The determination of the reasonableness of the denial of a request shall be made upon the initiation of an investigation by the NPC or upon the filing of a complaint, pursuant to the NPC's Rules of Procedure.

SECTION 11. ***Interpretation.*** **—** Any doubt in the interpretation of any provision of this Circular shall be interpreted in a manner mindful of the rights and interests of the data subject, and without prejudice to the application of other pertinent laws and regulations on the matter.

SECTION 12. ***Penalties.*** **—** The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA, its IRR, and related issuances of the NPC.

SECTION 13. ***Transitory Provisions.*** **—** PICs and PIPs shall be given a period of sixty (60) calendar days from the effectivity of this Circular to comply with the requirements provided herein.

SECTION 14. ***Separability Clause.*** **—** If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 15. ***Repealing Clause.*** **—** All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 16. ***Effectivity***. **—** This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner