Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Advisory No. 2020-04

DATE : 16 NOVEMBER 2020

SUBJECT : GUIDELINES ON THE USE OF CLOSED-CIRCUIT TELEVISION (CCTV) SYSTEMS

SECTION 1. ***General Principles.*** **—** This Advisory is governed by the following principles:

A. CCTV systems, where used reasonably and appropriately, are tools which support safety and security of personal information controllers (PICs), personal information processors (PIPs), and data subjects.

B. The use of CCTV systems shall consider its impact on the rights and freedoms of data subjects and be subject to regular review to ensure that its use remains to be necessary for specified and legitimate purposes.

C. The capture, use, retention, and destruction of video and/or audio footages obtained from CCTVs are considered as processing of personal data under the Data Privacy Act of 2012 (DPA). Those who process personal data through CCTV systems, whether as PICs or PIPs shall comply with the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR) and relevant issuances of the National Privacy Commission (NPC).

SECTION 2. ***Scope.*** **—**This Advisory shall apply to all PICs and PIPs engaged in the processing of personal data through the use of CCTV systems operating in public and semi-public areas. These include CCTV systems that record videos, as well as those systems with both video and audio capabilities.

SECTION 3. ***Definition of Terms.*** **—** Whenever used in this Advisory, the following terms shall have their respective meanings as hereinafter set forth:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

B. "Commission" or "NPC" refers to the National Privacy Commission;

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

D. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

E. "Masking" refers to concealing parts of the video or still imagery from view, which may include masking certain body parts or inanimate objects that could potentially disclose the identity of an individual. The common types of masking include solid color masked areas, where no details or movement in the scene covered by the masked area can be viewed, and blurred masking or pixelated masking, where the resulting images enables a partial outline to be seen but with detailed features obscured.[1]

F. "Personal information" refers to 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;

G. "Personal information controller" or "PIC" refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

   1. a person or organization who performs such functions as instructed by another person or organization; or
   2. an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

   There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

H. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.

I. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

J. "Public space" refers to a space that is generally open and accessible to the public, such as highways, streets, footbridges, overpass/underpass, parks, plazas, sidewalks, and other similar spaces;

K. "Semi-public space" refers to a space that, even if privately owned, is accessible to the public during operating hours. This include banks, educational institutions, hospitals, malls, offices, restaurants, transport stations, shops, and other similar establishments.[2]

SECTION 4. ***Guidelines.*** **—** The processing of personal data in CCTV systems shall be subject to the following guidelines:

[1] See: Singapore Personal Data Protection Commission, Advisory Guidelines on the PDPA for Selected Topics (revised 28 March 2017).
[2]See generally: Privacy Commissioner of New Zealand, *Privacy and CCTV: A Guide to the Privacy Act for Businesses, Agencies, and Organizations* (2009).

A. *Legitimate purpose*. Prior to installing a CCTV system, the purpose/s for personal data processing using such system must be clearly determined. Such processing may be permitted for the following purposes, except where the same are overridden by the fundamental rights and freedoms of the data subject:

1. Compliance with a law or regulation, where the same guarantees the protection of personal data;
2. Security of properties and protection of vitally important interests of individuals;
3. Ensure public order and safety; and
4. Other legitimate interests.

PICs shall identify an appropriate lawful basis for processing under the DPA and provide such basis when required by the Commission.

B. *Proportionality*. The PIC should evaluate whether the installation and operation of CCTV systems and the nature and kind thereof is necessary for its legitimate purpose, considering whether such purposes could be reasonably fulfilled by other less intrusive means.

Collection and further processing of personal data from CCTV systems should only be to the extent necessary to fulfill the legitimate purpose.

C. *Transparency*. PICs and PIPs shall provide CCTV notices which are readily visible and prominent within their premises, such as at points of entry, or other conspicuous areas. The CCTV notices shall provide information to the public that there is a CCTV system in operation in clear, plain, and concise language.

D. *CCTV policy*. PICs and PIPs are obliged to have a policy governing the operation of CCTV systems. Such policy shall provide details on the following:

1. Designation of an authorized personnel who shall have access to and responsibility for the operation, control, and monitoring of the CCTV system;
2. CCTV notice/s and placement thereof;
3. Procedure for requests for access to CCTV footages and providing a recording or copy thereof when requested that is consistent with the principles of these Guidelines;
4. Retention period of CCTV footages and manner of disposal/destruction thereof when period of retention has lapsed;
5. Security measures to be implemented for the protection of CCTV footages against any unlawful interference or interception, unauthorized access by copying, recording or viewing, accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing;
6. Conduct of regular evaluation and audit of security measures and whether the use of CCTV remains to be justified; and
7. Process for the regular review and assessment of the policy and its revision, if necessary.

E. *Location and placement*. To ensure that CCTV systems capture footages in a manner consistent with the DPA, the location and angles of the cameras must be carefully considered. CCTVs shall only be used to monitor the intended spaces, taking into consideration the purpose for monitoring the same.

The use of CCTVs in areas where individuals have a heightened expectation of privacy (*i.e.* fitting rooms, rest rooms, toilets, lactation or breastfeeding rooms, and other similar places) is prohibited.

F. *Quality and integrity of data*. CCTV systems shall record images that are of suitable quality to meet the purposes for which it was installed or intended. PICs shall implement reasonable and appropriate safeguards to ensure and maintain the integrity and accuracy of the footage recorded and stored, including any associated meta data (*i.e.* time, date, and location), and to facilitate access requests for CCTV footage.

G. *Obligations of PIPs*. Entities that operate CCTV systems on behalf of and under the instructions of PICs are considered as PIPs. As such, they shall likewise comply with all obligations under the DPA, its IRR, and other relevant issuances of the NPC. This includes, among others:

1. Process strictly in accordance with instructions from the PIC;
2. Implement organizational, technical, and physical security measures; and
3. Cooperate and coordinate with the PIC for access requests from data subjects or third parties.

H. *Privacy Impact Assessment.* A privacy impact assessment (PIA) helps a PIC determine that all CCTV cameras installed serve a legitimate purpose. It navigates the process of understanding the personal data flows in the organization. It identifies and provides an assessment of various privacy risks, and proposes measures intended to address them.

In determining the need to conduct a PIA for CCTV systems, the PIC should consider the size and sensitivity of the personal data being processed, the duration and extent of processing, the likely impact of the processing to the data subject, and possible harm in case of a personal data breach.

SECTION 5. ***Specific use cases.*** The use of CCTV systems shall be limited to and consistent with the purpose/s for which the same was established. The use of CCTVs may be for the following instances:

A. *Household.* Generally, the use of CCTV systems for purely personal, family or household affairs is outside the purview of this Advisory. Nonetheless, the use of these systems shall still bear in mind the rights of every individual to privacy.

Where a CCTV faces outwards from an individual's private property and it captures images of individuals beyond the boundaries of such property, particularly where it monitors a public space, the CCTV system cannot be considered as being for a purely personal, family or household purpose. As such, the operator of such CCTV system is deemed as a PIC and will be subjected to the obligations under the DPA and the provisions of this Advisory.

B. *Security*. The use of CCTVs as mandated by local government units (LGUs) for security and peace and order purposes is recognized. Reference can be made to the Department

of Interior and Local Government (DILG) Memorandum Circular No. 2014-119[3] on the requirement for the installation of CCTVs for certain business establishments and in strategic areas frequented by the public to support law enforcement and crime prevention, deterrence, detection, and solution efforts of the government.

C. *Employment.* The DPA recognizes that PICs have a legitimate interest to protect their assets, reputation, and business. To this end, PICs may monitor, through CCTVs, its premises and employees' use of company assets. Note, however, that employees do not lose their privacy rights in the workplace. Personal data of the employees shall only be collected, used, and stored by the employer, through CCTV monitoring, if the purpose sought to be achieved cannot be fulfilled by any other less privacy intrusive means.[4]

   The scope and terms of use of monitoring using CCTV in the workplace must be embodied in a company policy and the employees should be informed of the nature and extent of the monitoring specified in the said policy.

D. *Lawful surveillance*. Law enforcement agencies and other government agencies conducting lawful surveillance are not subject to the provisions of this Advisory. Nonetheless, the same shall be subject to the Constitution and other applicable laws and regulations.

Section 6. ***Storage and retention.*** Footage recorded by CCTV cameras shall be stored in a secure manner, whereby its confidentiality, integrity, and availability are maintained and protected. The recorded footage shall be encrypted.[5]

Access to the area where the CCTV footages are stored shall be secured and restricted to authorized personnel or persons only. Access logs for the CCTV footage shall be updated on a regular basis, including transfers, reproductions, and access requests.

Likewise, PICs should restrict monitoring of live CCTV feeds. It should identify responsible persons who are the only ones allowed to monitor such live feeds.

There is no specific or fixed minimum or maximum retention periods for CCTV footage. The same shall be retained only for as long as necessary to fulfill of the purposes for which the CCTV footage was obtained. Retention period shall not be determined based solely on the storage capacity of a system. Once determined, such information on retention period shall be clearly documented and form part of the CCTV policies.

SECTION 7. ***Data subject request for access.*** **—** Any person whose image is recorded on a CCTV system has a right to reasonable access and/or be supplied with a copy of their own personal data from the footage, subject to the provisions of Section 13 of this Advisory.

[3]Department of Interior and Local Government, Directing Cities/Capital Towns To Require The Installation Of Closed-Circuit Televisions (CCTV) For Certain Business Establishments In Accordance With Section 16 (General Welfare Clause) Of Republic Act No. 7160 To Support The Maintenance Of Peace And Order And Public Safety [Memorandum Circular No. 2014-119] (Sept. 15, 2014).
[4] See: National Privacy Commission, NPC Advisory Opinion No. 2018-084 and 2018-090.
[5] See: National Privacy Commission, Security of Personal Data in Government Agencies, Memorandum Circular No. 16-01 [NPC Circular 16-01] (October 10, 2016).

PICs shall establish policies and procedures allowing for such access and/or obtaining a copy, and shall consider the following:

A. Use of a standard form for requests for access: *provided,* that a request for access containing information sufficient to process the request should be acted upon even if a standard form is not used;
B. Verification of the identity of the individual requesting for access through the presentation and/or submission of supporting documentation: *provided*, that the required information is only to the extent necessary to confirm such identity;
C. For persons requesting access for and on behalf of another, the PIC may request for 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;
D. Purpose/s of the request for access, which should not be contrary to law, morals or public policy; and
E. Sufficient details on the requested footage such as the specific date/s, approximate time, location, among others, to enable the PIC to locate such footage.

Where images of parties other than the requesting data subject and/or the person/s sought to be identified as part of the request (e.g. identification of malefactors for investigation or law enforcement purposes) appear on the CCTV footage, legitimate interest under Section 12(f) of the DPA may apply as basis for disclosing, subject to Section 9 of this Advisory.

SECTION 8. ***Third party access request***. When a person, other than a data subject, requests for access to CCTV footage, it shall be treated as a third-party access request. The same policies and procedure as outlined in the previous section on data subject access request shall also be applicable.

PICs should decide on the merits of the request for disclosure based on its internal policy, the DPA, and other existing laws and regulations. Once a PIC has disclosed information to another, the latter becomes responsible for the copy they hold. It is their responsibility to comply with the DPA in relation to any further disclosures. The method of disclosing information should be secure to ensure they are only seen by the intended recipient.

CCTV footage may be disclosed for, but not limited to, the following purposes:

A. *Law enforcement and criminal investigations.* With respect to request for CCTV footage to be disclosed in relation to a criminal investigation, PICs shall require the law enforcement officer or the requesting party to provide sufficient proof as to the occurrence of a crime and the investigation thereof as well as proof of authority of the law enforcement officer before release of the CCTV footage.

   This request for CCTV footage shall be done following existing standard operating procedures in the conduct of an investigation and law enforcement operation as stated in the Revised PNP Operational Procedures, and other pertinent laws, rules, and regulations governing the same should be strictly adhered to.

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

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

D. *Request from the media.* PICs are not obliged to release CCTV footages to the media, unless there is a lawful basis for processing, and always with due regard to the rights of data subjects and codes of conduct and ethical standards of journalism.

   PICs are likewise proscribed from disclosing CCTV images of identifiable individuals to the media for entertainment purposes, unless it is with the consent of the said individuals. Law enforcement agencies may release CCTV footage to the media, on a case to case basis, considering the requirements of public order and safety, identification purposes, and other relevant factors.

   Where images of parties other than the requesting data subject and/or the person/s sought to be identified as part of the request (e.g. identification of malefactors for investigation or law enforcement purposes) appear on the CCTV footage, it is the responsibility of the requesting media personnel or journalist to mask the images of those other parties before making the footage public.

E. *Other third-party requests.* Third-party access requests for CCTV footage and images shall be approached with care as wider disclosure may be unfair to the individuals concerned. In certain circumstances, it may be appropriate to release information to a third party, where their needs outweigh those of the data subjects whose information is recorded. The PIC must determine on a case to case basis if it will accede to such request taking into consideration the rights and freedoms of the data subjects whose images are recorded by the CCTV system, and considering the provisions of the immediately succeeding section.

SECTION 9. ***Legitimate interest three-part test.*** In determining whether the data subject access request, in instances when the CCTV footage includes other data subjects, under Section 7, or the third-party access request under Section 8(E) may be allowed pursuant to legitimate interest as provided for under Section 12(f) of the DPA, the following shall be considered:

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

In this regard, CCTV footages requested for purposes of the protection of lawful rights and interests or the establishment, exercise or defense of legal claims under Section 13(f) of the DPA may be considered as legitimate interest.[6]

[6] KRL v. Trinity University, National Privacy Commission CID Case No. 17-K-003 (2019).

At all times, PICs shall be mindful that footage to be disclosed, either by viewing or providing a copy, are only those that are necessary and not excessive to the purpose for which they are being disclosed.

SECTION 10. ***Response procedure.*** **—** Once a PIC or a PIP is notified that a request for access is or will be made, the pertinent CCTV footage shall be taken out of the coverage of the usual retention period to enable the same to be saved and accessed.

Upon fulfillment of the requirements in the immediately preceding sections, the PIC response in allowing access to the CCTV footage shall be tiered: either by viewing or providing a copy to the data subject or the third party, as the case may be. The latter option shall be allowed when proportional to the purpose of the request.

A. *Viewing.* The requesting party may be allowed a reasonable opportunity to view the requested footage; *provided,* that CCTV footages shall be viewed in a secure area; *provided further,* that only the requesting party and the authorized personnel of the PIC shall be allowed to view such footages; *provided finally,* that other security measures to ensure confidentiality of the footage to be viewed may be implemented, such as signing of non-disclosure agreements or prohibiting the capture of the footage through mobile phones and other devices, where appropriate.

B. *Obtaining a copy of the CCTV footage.* If the requesting party opts to obtain a copy of the CCTV footage, PICs shall likewise provide the same. PICs shall ensure that the copying of footages is made in a secure manner that maintains the integrity of the footage and any associated meta data. Such process shall not interrupt the operation of the CCTV system.

   In circumstances where there is technical difficulty in providing a copy of the footage in video format, PICs may provide image stills as an alternative. Where image stills are provided, it would be necessary to supply sufficient stills for the duration of the requested footage.

SECTION 11. ***Fees and charges.*** **—** The PIC may charge the data subject or third party a reasonable fee for providing a copy of the footage to cover administrative costs: *provided*, that fees imposed shall not be excessive as to discourage such requests.

SECTION 12. ***Period for complying with the request.*** **—** PICs shall act on the request without undue delay, considering whether the request is for viewing only or obtaining a copy and the effort required on the part of the PIC to retrieve the requested information: *provided*, that the period shall not exceed fifteen (15) working days after receipt of the request and/or the necessary supporting or additional documentation when the request involves obtaining a copy, and shall not exceed five (5) working days when the request is for viewing only: *provided further*, that if a request is complex or numerous, compliance with such request may be extended for a period not exceeding another fifteen (15) working days: *provided finally*, that the data subject or his or her authorized representative is notified of the reason for the extension and the final date of release.

SECTION 13. ***Denial of request.*** **—** PICs may refuse to provide a copy of CCTV footages or access thereto in the following instances:

A. Incomplete information regarding the requested CCTV footage, as stated in Section 7;
B. 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;
C. Purpose for viewing or obtaining a copy of the footage is contrary to law, morals, or public policy;
D. The burden or expense of providing access would be unreasonable or involve disproportionate effort on the part of the PIC or PIP;
E. The footage has been deleted by the time the PIC receives the request, pursuant to its documented retention policy; or
F. If sharing the footage could put an ongoing criminal investigation at risk.

Should the PIC deny a request for CCTV access, it shall provide the requesting party with a justification for such denial.

SECTION 14. ***Reasonableness of the denial.*** **—** The determination of the reasonableness of the denial of a request shall be made by the NPC upon the filing of a complaint by the data subject pursuant to the NPC's rules of procedure.

SECTION 15. ***Interpretation.*** **—** Any doubt in the reasonableness of denying or limiting access to CCTV footages or the granting of the same shall be liberally interpreted in a manner that would uphold the rights and interests of the individual whose personal data is processed.

Approved:

SGD.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner