NPC Circular No. 2024 - ___

DATE : _____

SUBJECT : **GUIDELINES ON THE PROCESSING OF PERSONAL DATA COLLECTED USING BODY-WORN CAMERAS**

SECTION 1. ***Scope and Purpose***. — This Circular applies to personal information controllers (PICs) and personal information processors (PIPs) engaged in the processing of personal data through the use of Body-Worn Cameras (BWCs) and alternative recording devices (ARDs) and aims to establish protocols for the protection of individuals' personal data and their data privacy rights, ensuring accountability in personal data processing activities involving BWCs and ARDs.

SECTION 2. ***Definition of Terms***. — 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. "Alternative Recording Device" or "ARD" refers to an electronic camera system which is not a body-worn camera, that is capable of creating, generating, sending, receiving, storing, displaying, and processing audio-visual recording, and may be worn during law enforcement activities. It may be used as a substitute for body-worn cameras in case of unavailability.[1]

B. "Body-Worn Camera" or "BWC" refers to an electronic camera worn on the person of a law enforcement officer that is capable of creating, generating, sending, receiving, storing, displaying, and processing audio-visual recordings;[2]

C. "Data Custodian" refers to an officer of the law enforcement agency implementing the arrest or search warrant, who has the delegated responsibility of storing and safekeeping data recorded from body-worn cameras;

D. "Police Operations" refer to the categories of operations as defined under Rule 3 of the Revised Philippine National Police Operational Procedures:[3]

1. Public Safety Operation – includes Search, Rescue and Retrieval Operations, Fire Drills, Earthquake Drills and similar operations that promote public safety;
2. Law Enforcement Operation – includes Service of Warrant of Arrest,

[1] Supreme Court of the Philippines, Rules on the Use of Body-Worn Cameras in the Execution of Warrants [A.M. No. 21-06-08-SC], Rule 1, § 4 (1).
[2] Philippine National Police, "Operational Guidelines and Policies on the Use of Body Worn Camera [PNP Memorandum Circular No. 2018-009], § 4 (a) (March 15, 2018).
[3] Philippine National Police, Handbook PNPM-DO-DS-3-2-13, Revised Philippine National Police Operational Procedure, December 2013, *available at* http://www.pnp.gov.ph/images/Manuals_and_Guides/pop_manual_2013-1.pdf (last accessed 19 June 2021).

Implementation of Search Warrant, Enforcement of Visitorial Powers of the Chief, Philippine National Police and Unit Commanders, Anti-Illegal Drugs Operation, Anti-Illegal Gambling Operations, Anti-Illegal Logging Operations, Anti-Illegal Fishing Operations, Anti-Carnapping Operations, Anti-Kidnapping Operations, Anti-Cyber Crime Operations and similar operations that are conducted to enforce laws, statutes, executive orders and ordinances;

3. Internal Security Operation – includes Counter-Insurgency Operations, Counter Terrorist Operations and similar operations that are conducted to ensure internal security;
4. Special Police Operation – includes Checkpoint Operation, Roadblock Operation, Civil Disturbance Management Operation, Police Assistance in the Enforcement of Demolition Eviction Injunction and Similar Orders, Police Assistance in the Implementation of Final Court Order and Order from Quasi-Judicial Bodies, Hostage Situation, Visit Board Search and Seizure Onboard Marine Vessels and similar police operations that are conducted by police units with specialized training on the peculiarity of the mission or purpose;
5. Intelligence Operation – includes Surveillance Operation, Counter Intelligence, Intelligence Research, Intelligence Assessment and similar police intelligence operation conducted to gather information related to security, public safety and order;
6. Investigation Operation – includes Investigation of Crime or Incident, Administrative Investigation and similar investigative work necessary to determine facts and circumstances for filing cases criminally or administratively; and
7. Scene of the Crime Operation (SOCO) – includes the processing of crime scene, technical and forensic examination of evidence and similar scientific investigative assistance;

E. "Law Enforcement Agencies" or "LEAs" refer to persons engaged in police operations defined herein and other law enforcement functions, whether appointed, elected, or exercising delegated authority. These agencies include, but is not limited to, the Philippine National Police (PNP), Philippine Drug Enforcement Agency (PDEA), Land Transportation Office (LTO), Land Transportation Franchising and Regulatory Board (LTFRB), National Bureau of Investigation (NBI), Bureau of Immigration (BI), and Metropolitan Manila Development Authority (MMDA);

F. "Law Enforcement Officer" includes all officers of the law, whether appointed or elected, who exercise police powers, especially the powers of arrest or detention;[4]

G. "Metadata" refers to any digital identifiers that are captured as part of the actual recording, such as date, time, GPS coordinates, among others;[5]

H. "Private Security Agency" or "PSA" refers to any person, natural or juridical, who contracts, recruits, furnishes or posts any security guard, to perform its functions or solicit individuals, businesses, firms, or private, public or government-owned or -controlled corporations (GOCCs) to engage its service or those of its security guards,

[4] United Nations, Code of Conduct for Law Enforcement Officials, Adopted by General Assembly resolution 34/169 of 17 December 1979, available at https://www.ohchr.org/Documents/ProfessionalInterest/codeofconduct.pdf (last accessed 19 June 2021).
[5] PNP Memorandum Circular No. 2018-009, § 4 (d).

for hire, commission or compensation through subscription or as a consultant/trainer to any private or public corporation whose business or transactions involve national security or interest like the operation and/or management of domestic or ocean vessels, airplanes, helicopters, seaports, airports, heliports, landing strips among others or as consultant on any security related matter, or to provide highly specialized security, private escort, detective and investigation services like gangway security, catering security, passenger profiling, baggage examination, providing security on board vessels or aircraft, or other security needs that the PNP may approve;[6]

I. "Recording" refers to any digital material generated as a result of using body-worn cameras which contains images, audio, and video footages.[7]

SECTION 3. ***Principles; lawful basis for processing***. — The processing of personal data through BWCs or ARDs shall be subject to the following requirements.

A. *Law enforcement; security*. BWCs or ARDs shall be used in a manner consistent with the aim of ensuring the protection of the fundamental rights and freedoms of all data subjects, including law enforcement officers and security guards. Personal data processing of LEAs and PSAs shall adhere to the following:

1. *Lawful basis for processing*. The processing of personal data using BWCs or ARDs may be allowed in any of the instances provided under Sections 12 and 13 of the DPA, or as processing under a special case under Section 4 of the DPA.

2. *General principles of privacy*. The general data privacy principles shall be strictly adhered to:

a. Transparency. An appropriate privacy notice shall be provided using clear, concise, and plain language, considering the different contexts and environments where personal data processing could take place.

i. The privacy notice shall be translated into Filipino or another language or dialect to allow it to be better understood by data subjects;
ii. The privacy notice shall be published prior to the use of BWCs or ARDs and thereafter placed or made available in a conspicuous or easily accessible place;
iii. Such privacy notice shall likewise be incorporated in the guidelines on the use of BWCs or ARDs which shall also be readily accessible and published; and
iv. In certain limited instances, information on the processing of personal data using BWCs or ARDs may be given to data subjects at the next practical opportunity.

b. Legitimate purpose. The processing of personal data shall be compatible with a declared and specified purpose which must not be contrary to law, morals,

[6] An Act Strengthening The Regulation Of The Private Security Services Industry, Repealing For The Purpose, Republic Act No. 5487, Entitled "Ac Act To Regulate The Organization And Operation Of Private Detective Watchmen Or Security Guard Agencies", As Amended [The Private Security Services Industry Act] Republic Act No. 11917 (2022).
[7] Supreme Court of the Philippines, Rules on the Use of Body-Worn Cameras in the Execution of Warrants [A.M. No. 21-06-08-SC], Rule 1, § 4 (5) (June 29, 2021).

or public policy. The use of BWCs or ARDs may be permitted for the following purposes:

i. In any of the instances provided in Section 6 (b) (3) of the PNP Operational Guidelines and Policies on the Use of Body Worn Camera;[8]
ii. Security of property and protection of vitally important interests of individuals; and
iii. To ensure public order and safety.

c. Proportionality. The processing of personal data through the use of BWCs or ARDs shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. The collection and further processing of personal data through BWCs or ARDs should only be to the extent necessary to fulfill the legitimate purpose.

d. Fairness and lawfulness. The processing of personal data using BWCs or ARDs shall not be unduly oppressive upon data subjects. Personal data processing activities shall comply with the Rules on the Use of Body-Worn Cameras in the Execution of Warrants issued by the Supreme Court, and other laws, rules or regulations.

B. *Other persons or entities using BWCs and ARDs*. The processing of personal data through the use BWCs and ARDs for purposes other than law enforcement, police operations, or security, such as for training, quality control, monitoring, and other related purposes, shall be subject to the same requirements in Section 3 (A) above on having a lawful basis for processing and adherence to the general principles of privacy.

SECTION 4. ***Security measures.*** **—** PICs and PIPs shall implement reasonable and appropriate organizational, technical, and physical safeguards, considering the need to maintain confidentiality, integrity, and availability of personal data collected through BWCs or ARDs. These safeguards shall include the following:

A. Providing for the conduct of comprehensive trainings or seminars for all relevant personnel on the proper use of BWCs or ARDs:

1. Training materials shall include discussions on the right to privacy, data protection policies, general data privacy principles, rights of the data subjects, and compliance with due process requirements as provided by law;
2. Training materials shall also include a discussion of administrative, civil, and criminal penalties for unauthorized use and disclosure of recordings and any other personal data; and
3. Trainings shall be properly documented and conducted at least once a year: *provided*, that a similar training shall be provided during the onboarding or orientation of newly hired personnel.

B. Regulating access to personal data collected through BWCs or ARDs:
1. Only authorized personnel shall have access to recordings. For this purpose, authorized personnel shall be appointed or designated, taking into consideration

[8] PNP Memorandum Circular No. 2018-009, § 6 (b).

the following:

a. Supreme Court Rules on the Use of Body-Worn Cameras in the Execution of Warrants, specifically Rule 4 requiring data custodians and prescribing rules on downloading data, preservation of metadata, chain of custody, custody and access to recordings, among others;
b. PNP Operational Guidelines and Policies on the Use of Body Worn Camera, specifically the provisions on Post-Operations Phase requiring downloading and storage of recorded data and the PNP personnel in charge of storage, review, disclosure, and monitoring and audit of recordings.
c. NPC Advisory No. 2021 – 01 on Data Subject Rights, specifically on general policies and procedures in upholding data subject rights.

2. Implementing an access control policy that would prescribe the processes and procedures on the access of recorded data. In all instances where access is allowed, the same should be covered by a security clearance or similar authorization, a copy of which shall be filed with the PIC's data protection officer. The process for the issuance of security clearances or similar authorizations shall be documented in the access control policy.

3. Requests for access by any person whose image is recorded on BWCs or ARDs as well as third party access requests shall be governed by the procedures provided under the NPC guidelines on Closed-Circuit Television (CCTV) Systems.

C. Ensuring that the BWCs or ARDs have the following features:[9]

1. The recordings shall be in a standard, open, non-proprietary format such that it can be replayed in a freely available software;
2. The device exports all recordings to data archiving/management system in its original file format and without loss of quality or associated metadata;
3. The device prohibits recordings from being edited or deleted, except through a data management software once recordings have been transferred, and should not overwrite existing data before they have been transferred. The recorded data transferred to an external media storage device should also be protected from editing or deletion until it is no longer necessary for the fulfillment of the purposes for which the data was obtained.
4. Require recordings to contain a date (*e.g.*, month:day:year) and time stamp (*e.g.*, hours:minutes:seconds) capable of being exported with the imagery in a format that is readable in third party software; and
5. Presence of a visual recording indicator that is clearly visible to those being recorded.

D. Safeguarding recordings during storage and transmission using appropriate encryption software.

E. Establishing a policy governing the process of downloading, transmitting, and storing recordings on another device, which will be used to facilitate access requests from the data subject.

[9] See generally: United Kingdom, Home Office Centre for Applied Science and Technology, Body-Worn Video Technical Guidance, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/565608/body-worn-video-technical-guidance-1414.pdf (last accessed 21 June 2021).

F. Retain recordings only for as long as necessary for the fulfillment of the purposes for which the data was obtained, the establishment, exercise, or defense of legal claims, or as provided by law:

1. Recordings shall be retained for sixty (60) days or as may be provided for in other laws or regulations that may require its retention: *provided*, that those recordings that are necessary for pending investigations, prosecutions, or cases with judicial or quasi-judicial bodies, or to be used for training PNP personnel[10] may continue to be processed in accordance with the applicable criteria for lawful processing under Sections 12 and 13 of the DPA or the special cases under Section 4 of the DPA, and retained for a longer period, subject to appropriate safeguards. This provision shall not be construed as limiting or denying data subject access requests which have been made before the lapse of the sixty (60)-day period; and
2. Recordings shall be disposed in a secure manner that would prevent unauthorized further processing. The storage media must be electronically wiped, including back up data, to ensure that recordings are permanently erased and beyond recovery.

SECTION 5. ***Upholding data subject rights.*** — Mechanisms for data subjects to exercise their rights under Sections 16 to 18 of the DPA shall be provided.

A. The exercise of such rights is subject to reasonable limitations, such as when upholding data subject rights would prevent, impair, or otherwise prejudice ongoing police operations and other related law enforcement activities, or in the interest of national security or public order or safety, as may be provided for by law: *provided,* that when the identified reasonable limitations herein have ceased to exist, the data subject rights should subsequently be upheld, *e.g.*, in case of an access request which was denied as it may affect ongoing police operations, the specific footage requested should be tagged, archived, and released when such action would no longer prevent, impair, or otherwise prejudice ongoing police operations.

B. Data subjects shall informed that they are being recorded unless doing so would be impractical, dangerous, or impossible for the specific police operation, other law enforcement activity, or analogous circumstances.

1. Nevertheless, PICs are required to inform the data subjects with relevant information at the next practical opportunity which depends upon the surrounding circumstance of the case.
2. The timing of the provision of information must always be within a reasonable period to give effect to the data subject's right to be informed.[11]

C. There shall be a careful determination and evaluation on whether the right to access to recordings may be granted depending on the circumstances such as when providing access to the requested recording may put an ongoing police operation at risk. In all cases, PICs shall be required to state the reason for the delay on granting or acting upon the requested access or the justification for the denial of the request.

[10] PNP Memorandum Circular No. 2018-009, § 6 (c) (2) (i) and (5) (a).
[11] See: ECA v. XXX, NPC Case No. 18-103 (2020).

SECTION 6. ***Privacy Impact Assessment***. — PICs shall conduct a privacy impact assessment (PIA) prior to the adoption, use, or implementation of BWCs or ARDs or within a reasonable time thereafter as may be determined by the concerned PICs. PIAs shall likewise be conducted when there are changes in the governing law or regulations or other proposed modifications affecting personal data processing through BWCs.

SECTION 7. ***Regular review and assessment.*** — PICs, through their data protection officers, shall conduct regular review and assessment of internal policies and security measures implemented in relation to the processing of personal data using BWCs or ARDs. The determination of the regularity of reviews and assessments shall be the responsibility of the PICs, taking into account new technologies, appropriate standards, and data privacy best practices.

SECTION 8. ***Interpretation***. — Any doubt in the interpretation of any provision of this Circular shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects, and without prejudice to the application of other pertinent laws and regulations on the matter.

SECTION 9. ***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 10. ***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 11. ***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 12. ***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 13. ***Effectivity***. — This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy Commissioner