NPC Circular No. 2025 - 01

DATE : **26 May 2025**

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). This Circular aims to establish protocols for the protection of data subjects' personal data and their data privacy rights, ensuring accountability in personal data processing activities involving BWCs and ARDs.

A. The use of BWCs or ARDs for purely personal, family, or household affairs shall be outside of the scope of this Circular. Nonetheless, the use of BWCs or ARDs in these instances shall still bear in mind the rights of every individual to data privacy.

B. For purposes of this Circular, purely personal, family, or household affairs refer to the uses that are not intended for profit or commercial gain and where footages are not uploaded, posted, published or otherwise shared online. This includes the use of BWCs or ARDs by individuals, *e.g.*, motorcycle drivers, bicyclists, etc., for personal security purposes. Nevertheless, the totality of the circumstances surrounding the use of BWCs or ARDs will be considered in determining whether the specific activity falls under the exception.

   The following factors may be considered in determining whether a specific 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; and
   3. Processing of personal data about data subjects who have no personal, family, or household relationship with the person engaged in the processing.[1]

SECTION 2. ***Definition of Terms***. — Terms used in the Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations (IRR), as amended, and other NPC issuances, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

[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).

A. "Alternative Recording Device" or "ARD" refers to an electronic device or gadget with a camera system, other than a BWC, that is capable of creating, generating, sending, receiving, storing, displaying, and processing audio-visual recording and is capable of being bodily worn, handheld, attached to the person of an individual or operated as an alternative or substitute for BWC. This includes, but is not limited to, digital cameras, mobile phones, action cameras, smart watches or smart eyeglasses, and other similar devices.

B. "Body-Worn Camera" or "BWC" refers to an electronic camera worn by a person that is capable and intended for creating, generating, sending, receiving, storing, displaying, and processing audio-visual recordings;

C. "Data Custodian" refers to an officer or personnel formally designated by the Personal Information Controller (PIC) to be responsible for the secure storage, safekeeping, access control, and overall management of personal data, including audio-visual recordings and metadata, generated through BWCs and ARDs;

D. "Police Operations" refer to the categories of operations as defined under Rule 3 of the Revised Philippine National Police Operational Procedures:[2]

1. Patrol Operations – the most basic police function and known as the backbone of policing;
2. Law Enforcement Operation – include service of warrant of arrest, implementation of search warrant, enforcement of visitorial powers of the Chiefs of Police, and other anti-criminality operations;
3. Internal Security Operation – include counterterrorism operations and similar operations against other threat groups that are conducted to ensure internal security;
4. Public Safety Operations - include critical incident management procedures, search, rescue and retrieval operations, hostage situation, civil disturbance management operation, management of health hazards and other operations that promote public safety;
5. Special Police Operations - include high-risk checkpoint and roadblock operation, police assistance in the implementation of order from the court and other quasi-judicial bodies, security to major and special events, aircraft hijacking operations, visit, board, search and seizure of marine vessels, and similar police operations that are conducted by police units with specialized training on the peculiarity of the mission or purpose;
6. Investigation Operations - include investigation of crime or incident, Scene of the Crime Operations (SOCO), administrative investigation and other investigative work necessary to determine facts and circumstances for filing cases criminally or administratively;
7. Police Community Relations – include three interrelated dimensions to accomplish its mission namely: community affairs and development, public information, and information development operations to forge partnership and strengthen collaboration and linkages with the community;

[2] Philippine National Police Manual PNPM-DO-D-0-2-13-21, Revised Philippine National Police Operational Procedure, September 2021, *available at* https://akg.pnp.gov.ph/wp-content/uploads/2024/01/POP-Manual-2021.pdf (last accessed October 21, 2024).

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 are 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), Bureau of Internal Revenue (BIR), Bureau of Customs (BOC), and Metropolitan Manila Development Authority (MMDA);

F. "Law Enforcement Officer" includes all officers of the law, whether appointed, delegated, deputized, or elected, who exercise police powers, especially the powers of arrest or detention;[3]

G. "Metadata" refers to any digital identifiers that are captured as part of the actual recording, such as date, time, GPS coordinates, among others;[4]

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, 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;[5]

I. "Recording" refers to any digital material generated as a result of using BWCs or ARDs which contains images, audio, and video footages;[6]

J. "Vlogger" refers to someone who makes video blogs or vlogs (recording of thoughts, ideas, or opinions on a subject) and posts them on the internet.[7]

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

[3] See generally: 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).
[4] PNP Memorandum Circular No. 2018-009, § 4 (d).
[5] 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).
[6] 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).
[7] See: Cambridge Dictionary entry for vlogger, available at https://dictionary.cambridge.org/us/dictionary/english/vlogger (last accessed Jan. 10, 2025).

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. PICs shall consider the following in presenting their privacy notice:
            1. Place visible signage on the person of the law enforcement officers and security guards, or a warning light on the BWCs or ARDs to indicate that the device is activated and recording;[8] and
            2. Provide data subjects a published privacy notice, or direct them to a privacy notice placed or made available in a conspicuous or easily accessible place, *e.g.*, website, office premise, etc.

        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, or public policy. The use of BWCs or ARDs may be permitted for the following purposes, as such but not limited to:

        i. In any of the instances provided in the PNP Operational Guidelines and Policies on the Use of Body Worn Camera and relevant issuances of the PNP;[9]
        ii. Enforcement of traffic laws, rules and regulations;
        iii. Security of property and protection of life and interests of individual; and
        iv. To ensure public order and safety.

[8] See generally: UK Information Commissioner's Office, *Additional considerations for technologies other than CCTV - Body Worn Video (BWV)*, available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/additional-considerations-for-technologies-other-than-cctv/?q=children#bwv (last accessed: 2 September 2024).
[9] PNP Memorandum Circular No. 2018-009, § 6 (b).

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 applicable laws, rules or regulations.

B. *Vlogging.* Vloggers who use BWCs or ARDs to capture the image, audio, or video of persons for uploading, posting, publishing or otherwise sharing online may be deemed to be engaged in the processing personal data.

1. *Lawful basis for processing*. Vloggers may generally rely on Section 12 (f) of the DPA as a lawful basis for processing: *provided,* that in certain specific instances where sensitive personal information is captured, vloggers need to have a lawful basis under Section 13 of the DPA.

2. *Transparency; fairness*. In the scenario where vloggers are recording footage of themselves in action, *e.g.*, eating, shopping, driving, biking, dancing, walking, or otherwise engaged in general video recording activities in public or semi-public places which may capture audio-visual information of bystanders or other people, vloggers shall ensure that that personal data processing activities are done in a fair and lawful manner and affected data subjects will be able to exercise their rights.

a. Generally and where appropriate in given scenarios, *e.g.,* interviewing specific individuals, vloggers shall ensure transparency and provide adequate information to the data subjects prior to the commencement of any video recording activity, including the fact that the resulting footage will be uploaded, posted, published or otherwise shared online, and how they may exercise their data privacy rights.

b. Vloggers shall have an appropriate privacy notice on all online platforms which shall provide details to affected data subjects on how to exercise their right to object, right to erasure, take down of posts, among others.

c. Vloggers are required to use available technology that can mask images of bystanders, especially children and other vulnerable individuals.

C. *Other persons or entities using BWCs or ARDs*. The processing of personal data through the use BWCs or ARDs for purposes other than law enforcement, police operations, or security, such as for training, quality control, monitoring, assessment, evaluation, audit, and other related purposes, shall be subject to the same requirements on having a lawful basis for processing, adherence to the general principles of privacy, implanting safeguards, and upholding data subject rights.

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 data 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 under the DPA; 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 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 or by any further issuance of the Commission.

C. Ensuring that the BWCs or ARDs have the following features:[10]

[10] 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).

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), time stamp (*e.g.*, hours:minutes:seconds), and location data, 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.

F. Retain recordings only for as long as necessary for the fulfillment of the purposes for which the data was obtained:

1. *Law enforcement and public authority.* Recordings that are necessary for pending investigations, prosecutions, or cases with judicial or quasi-judicial bodies, or to be used for training PNP personnel[11] 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 thirty (30)-day period.

2. *Retention of recordings by other persons or entities using BWCs or ARDs*. Recordings made by persons or entities shall be retained for thirty (30) calendar days or as may be provided for in other laws or regulations that may require its retention.

3. *Disposal of recordings.* 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.

[11] PNP Memorandum Circular No. 2018-009, § 6 (c) (2) (i) and (5) (a).

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 may exercise their rights with due consideration of the rights and freedoms of others, *e.g.*, in case of an access request for footage which captures other individuals who are irrelevant to the purpose of the request, PICs must mask the images of those other individuals prior to the release of such footage.

C. Data subjects shall be 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. 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.[12]

D. 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.

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, and any other issuances to be released by the Commission affecting personal data processing through BWCs or ARDs. PIAs shall be regularly reviewed.

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

[12] See: ECA v. XXX, NPC Case No. 18-103 (2020).

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:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

SGD.
JOSE AMELITO S. BELARMINO II
Deputy Privacy Commissioner