



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2022-019¹**

21 September 2022

[REDACTED]

Re: USE OF BODY-WORN CAMERA BY SECURITY PERSONNEL

Dear [REDACTED]:

We respond to your request for an advisory opinion regarding the use of body-worn cameras (BWCs) by the security personnel of ON Semiconductor Philippines, Inc., ON Semiconductor SSMP Philippines Corporation, and ON Semiconductor Cebu Philippines, Inc. (collectively, Corporations).

We gather that the Corporations are affiliate companies located in Cavite, Tarlac, and Cebu, engaged in various manufacturing, processing, and sale of semiconductors. Currently, the Corporations are exploring the possibility of requiring their security personnel to use body-worn cameras to record their field observations and encounters, on top of the use of closed-circuit television systems (CCTVs).

You thus ask whether the Corporations' security personnel can employ BWCs without violating the provisions of the Data Privacy Act of 2012² (DPA).

*Lawful basis for processing personal information;
Section 12;*

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.³

¹ Tags: body-worn cameras, lawful processing of personal information; general data privacy principles; transparency; proportionality; privacy notice.

² An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for r-this Purpose a National Privacy Commission, and for other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Data Privacy Act of 2012, § 4.

Personal information is defined as 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.⁴

Consequently, under the DPA, the images of identifiable individuals captured in a photograph or audiovisual recordings are considered personal information⁵ about the individual. Thus, the processing of which should comply with the provisions of the DPA.⁶

You mentioned that the use of the BWCs will be for a legitimate purpose, *i.e.*, to promote the safety and protect the security of people and the manufacturing facilities of the Corporations. The use of BWCs is envisioned to:

1. Raise standards during confrontational incidents
2. Improve efficiency in incident escalation
3. Supplement opportunities for evidence capture
4. Reduce complaints
5. Assist with disciplinary and/or legal proceedings.

As justification, you cited Section 12 of the DPA, which provides for the criteria for lawful processing of personal information based on legitimate interests of the personal information controller (PIC), *to wit*:

SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: x x x

(f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

At the outset, we acknowledge that employers have legitimate standing to uphold its legitimate business interests, such as employee monitoring, security of the premises, investigations or disciplinary purposes, and other reasonable purposes which are not contrary to law, morals, or public policy.

However, we emphasize that legitimate interest in the processing activity should be linked to a specific context and that the PICs must determine the most appropriate lawful basis for processing personal information in relation to the specific purpose of the processing activity.

Hence, while the processing of personal information based on the legitimate interests of the PICs is allowed under the DPA, the Corporations must assess if the use of BWCs within the premises will pass the three-part test of Legitimate Interest, namely:

⁴ Data Privacy Act of 2012, § 3 (g).

⁵ *Id.* § 3 (g).

⁶ *Id.* § 3 (j).

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve.
2. 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
3. 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.

Adherence to the general data privacy principles; transparency; proportionality; privacy notice

Aside from determining the most appropriate lawful basis for processing, the Corporations must also adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality.

Particularly, the principle of proportionality requires that processing of personal information shall be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.⁷

As mentioned, the Corporations have CCTVs installed in their respective facilities. Considering all attendant circumstances, the Corporations must first conduct an assessment that the use of additional BWCs is truly necessary and is the least privacy intrusive manner of processing in relation to the declared purpose.

After evaluation, if the Corporations decide to use BWCs, they must ensure that the data subjects are informed that their security personnel are equipped with BWCs. This may be done through an appropriate privacy notice which you ensure will be complied with.

The privacy notice should describe the specific processes relating to the use of BWCs. In crafting the privacy notice regarding the use of BWCs, reference can be made to Section 16 (b) of the DPA on the information that should be provided to the data subjects pursuant to their right to be informed and to demonstrate the Corporations' adherence to the data privacy principle of transparency.

Further, the Commission, in the case of JVA vs UPeso⁸, ruled that:

The test to determine if the personal information controller has complied with the general privacy principle of transparency is to examine whether an average member of the target audience could have understood the information provided to them. x x x

If the data subjects would not be able to understand the information provided in the Privacy Notice, then the Corporations should translate their Privacy Notices into the language or

⁷ Data Privacy Act of 2012, § 11 (c).

⁸ National Privacy Commission, JVA vs UPESO [NPC Case No. 19-498] 9 June 2020

dialect understandable by the data subjects in their regions of operations so the latter may be fully informed of such processing.

The Corporations may also wish to review, among others, the instances when their security personnel will turn on their BWCs, the manner by which to immediately notify the data subjects on the use of BWCs, and the mechanism for data subjects to exercise their data privacy rights in relation to the BWC footages.

Privacy impact assessment

Finally, we recommend conducting a privacy impact assessment (PIA) on the use of BWCs to identify potential privacy risks to the data subjects.

A PIA is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or a personal information processor (PIP). It considers the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations.⁹

The PIA will help identify and provide an assessment of various privacy risks, and propose measures intended to address and mitigate the effect of these identified risks on the data subjects. We trust that after the conduct of a PIA, the Corporations would best be able to determine if the use of BWCs aligns with the basic data privacy principles.

Please be advised that this Advisory Opinion was rendered based solely on your provided information. Any extraneous fact that may be subsequently furnished to us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

Sgd.
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

⁹ NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.