Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-018[1]

18 June 2021

[redacted]

Re: PNP REQUEST FOR PERSONAL INFORMATION FROM EMPLOYERS

Dear [redacted],

We write in response to your request for advisory opinion on whether an employer may disclose the residential address, among others, of its current and/or former employees to law enforcement agencies serving warrants of arrest without violating the provisions of the Data Privacy Act of 2012[2] (DPA).

We understand that there have been instances wherein law enforcement agencies, such as the Philippine National Police (PNP), would come to the company premises to serve warrants of arrest on current and/or former employees.

We understand further that sometimes, these employees are not present in the company premises or not anymore connected with the company when the law enforcement officers try to serve the warrants, thus prompting the latter to request for the residential address, among others, of these employees so they may properly serve the same.

You now seek clarification whether you may disclose personal information of your current and/or former employees to the PNP without violating the DPA.

Scope of the DPA; special cases; fulfillment of mandates

Section 4 of the DPA provides that the DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing. Processing refers to any operation or any set of operations performed upon personal information

[1] Tags: law enforcement agencies; special cases; lawful processing of personal information; fulfillment of mandate; processing based on laws and regulations; general data privacy principles
[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.[3]

Further, Section 4 (e) of the DPA provides that the processing of information necessary to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement, subject to restrictions provided by law, is one of the special cases where the application of the provisions of the DPA and its Implementing Rules and Regulations (IRR) is qualified or limited.

This means that when the personal information is needed to be processed by a public authority, such as the PNP, pursuant to its statutory mandate, the processing of such personal data is may be allowed under the DPA and its IRR, to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.

The following should guide the company in relation to the above-quoted provision:

a) The information is necessary in order to carry out the law enforcement functions. Where the processing activity violates the Constitution, or any other applicable law, the processing will not be considered necessary for law enforcement purposes;
b) The processing is for the fulfillment of a constitutional or statutory mandate; and
c) There is strict adherence to all due process requirements. Where there is a nonconformity with such processes, such processing shall not be deemed to be for a special case.

PNP mandate; powers and functions

We understand that the PNP has the power and function under Section 24 of Republic Act No. 6975 or the Department of the Interior and Local Government Act of 1990,[4] to investigate and prevent crimes, effect the arrest of criminal offenders, bring offenders to justice, and assist in their prosecution, among others.

In addition, the Chief of the PNP and the Director and the Deputy Director of the Criminal Investigation and Detection Group (CIDG) have been granted subpoena powers under Section 1 of Republic Act No. 10973[5] to issue subpoena and subpoena duces tecum in relation to its investigation.[6]

The subpoena shall state the nature and purpose of the investigation, including a reasonable description of the books, documents, or things demanded which must be *relevant to the investigation.*[7]

Hence, as a general rule, it may be prudent for a personal information controller (PIC) to provide personal information to the PNP after it receives a formal subpoena to ensure that the PNP's request is authorized, proper, and lawful under existing laws and regulations. As previously stated, RA No. 10973 requires that the subpoena must state the personal information being requested, the reason for such request, and the relevance of the said request to the investigation being conducted.

[3] Data Privacy Act of 2012, § 3 (j).
[4] An Act Establishing the Philippine National Police under a Reorganized Department of the Interior and Local Government, and for Other Purposes [Department of the Interior and Local Government Act of 1990], Republic Act No. 6975, § 24 (1990).
[5]An Act Granting the Chief of the Philippine National Police (PNP) and the Director and the Deputy Director for Administration of the Criminal Investigation and Detection Group (CIDG) the Authority to Administer Oath and to Issue Subpoena And Subpoena Duces Tecum, amending for the Purpose Republic Act No. 6975, as amended, otherwise known as the "Department Of The Interior And Local Government Act Of 1990, Republic Act No. 10973, § 1 (2018).
[6] Ibid.
[7] Ibid.

In this case, however, although there is no subpoena from the PNP requesting for personal information, there is already an existing arrest warrant against the employees, thus, accommodating the PNP's request may be warranted under the DPA.

Nevertheless, the company is not precluded to further ask and/or confirm from the PNP additional details with respect to the validity of the warrant and the standard operating procedure to be followed in case the person to be arrested is not within the premises. The company should likewise keep documentation of such instances of disclosure of personal information in relation to law enforcement activities.

We emphasize that the DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly constituted public authorities. The DPA does not prohibit government agencies from processing personal data pursuant to their respective mandates, taking into consideration the applicable provisions of law, rules and regulations, and the general data privacy principles enunciated in the DPA.

General data privacy principles; proportionality

We wish to reiterate that while there may be lawful basis for processing under the DPA in this case, the company, as a PIC must always adhere to the data privacy principles of transparency, legitimate purpose, and proportionality.

Specifically, for proportionality, the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose and personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[8]

In keeping with the proportionality principle of the DPA, it is prudent to determine what particular personal data should be released to the PNP to aid the latter in the execution of the warrant of arrest.

The company should judiciously assess the request for information and the types of personal information being requested, if the same are proportional to the purpose of serving a warrant of arrest. Personal information not indispensable to such purpose need not be disclosed to law enforcement agencies.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).