Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-007[1]

5 March 2021

[redacted]

Re: DATA SHARING ARRANGEMENTS OF THE PHILIPPINE VETERANS AFFAIRS OFFICE WITH OTHER GOVERNMENT AGENCIES

Dear [redacted]

We write in response to your letter received by the National Privacy Commission (NPC) requesting for an Advisory Opinion on the various issues and concerns relating to data sharing of the Philippine Veterans Affairs Office (PVAO) with other government agencies.

We understand that PVAO is mandated under Republic Act (R.A.) No. 6948, as amended by R.A. No. 7696, otherwise known as An Act Standardizing and Upgrading the Benefits for Military Veterans and their Dependents, to ensure the qualifications of the pension applicants through the determination of the authenticity, validity, and credibility of the documents and information submitted to them. PVAO is also mandated to continuously monitor the status of the pensioners to ensure that they are still alive and whether their surviving spouses have remarried.

We understand further that PVAO has partnered with various government agencies to facilitate the verification of information of pensioners:

1. For information on pensioners on whether living or deceased, current civil status of a pensioner's surviving spouse and current address.
    a. Civil Registrar Office (CRO), through the local government and with the assistance of the Department of the Interior and Local Government (DILG):
    b. Philippine Statistics Authority (PSA); and
    c. Philippine Postal Corporation (PhilPost)
2. For military service records:

[1] Tags: data sharing; data sharing agreement; public function; fulfillment of lawful mandate; general data privacy principles.

a. Office of the Adjutant General – Non-Current Records Division (OTAG – NRD) and
b. Major Services Pension Gratuity Branch AFP

In this regard, you now seek clarification on the following matters:

1. Since the local civil registry (LCR) is under the control and supervision of their respective local government units (LGUs) and the latter are under the jurisdiction of the DILG, can PVAO enter into a Memorandum of Agreement/Understanding and data sharing agreement (DSA) with DILG rather than entering into several DSAs with each and every LCR?

2. PVAO, to ensure the authenticity of documents and determine the present status of the pensioner, uses the "record-deceased" submitted to it by PSA to check if any of those listed are PVAO claimants. This was restricted upon the enactment of the DPA. Does this arrangement require a DSA between PVAO and PSA?

3. To perform its mandate, PVAO has been requesting information from the LCR, PSA, and OTAG-NRD which were created to serve as the depository of information for the government. In line with this, the following queries were raised:

    a. Is PVAO still considered a third party for the purpose of data sharing with the aforesaid government agencies?
    b. Is it safe to say that information provided by the data subjects to the aforesaid government agencies be used and processed by the government in general, so that all government agencies may process the information as long as it is in accordance with their mandated functions?
    c. Further, are government agencies sharing data with other government agencies pursuant to the performance of their functions still need to comply with the requirements of the Data Privacy Act of 2012[2] (DPA)?

4. Are information shared among offices under the Department of National Defense (DND), such as the Armed Forces of the Philippines (AFP) and PVAO considered data sharing?

To address the foregoing concerns, we provide the following clarifications:

Data sharing; data sharing agreements; adherence to general data privacy principles

Data sharing is the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controller/s (PICs).[3] A data sharing agreement or DSA refers to a contract, joint issuance or any similar document which sets out the obligations, responsibilities and liabilities of the PICs involved in the transfer of personal data between or among them, including the implementation of adequate standards for data privacy and security and upholding the rights of the data subjects.[4]

[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).
[3] National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03], § 2 (F) (23 December 2020).
[4] *Id.* § 2 (g).

All data sharing arrangements, whether or not covered by a DSA, are governed by the following principles:

a. Adherence to the data privacy principles of transparency, legitimate purpose, and proportionality;
b. Fulfillment of all applicable requirements prescribed by the DPA, its Implementing Rules and Regulations (IRR) and other issuances of the NPC;
c. Recognition of upholding the rights of affected data subjects, unless otherwise provided by law;
d. Ensuring that the shared and collected data are accurate, complete, and where necessary for the declared, specified and legitimate purpose, kept up to date; and
e. Implementation of reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure as well as against any other unlawful processing.[5]

In this regard, any data sharing between or among government agencies are still required to strictly adhere to the foregoing principles. Needless to say, these data sharing arrangements involving government agencies are expected to be pursuant to their respective lawful mandates and official functions.

Government agencies; processing based on constitutional or statutory mandate

We reiterate that processing personal data pursuant to the fulfillment of a government agency's mandate or when the processing is provided for by existing laws and regulations are recognized under the various provisions of the DPA.[6] However, this does not mean that government agencies are already exempted from complying with all other provisions of the DPA, since the requirements of the DPA are not limited to having lawful basis in the processing of personal data.

Stated differently, although government agencies may have legal bases for the processing of personal data, such processing must still adhere to the other requirements of the law. As PICs, government agencies are required to, among others, implement safeguards to ensure the protection of personal data as well as the rights of data subjects.

Parties to a DSA; personal information controllers

Regarding your first query as to who may be the proper party to the DSA with the LCRs, we wish to clarify that the execution of a DSA under the latest NPC issuance is not mandatory:[7]

> "SECTION 8. Data sharing agreement; key considerations. — Data sharing may be covered by a data sharing agreement (DSA) or a similar document containing the terms and conditions of the sharing arrangement, including obligations to protect the personal data shared, the responsibilities of the parties, mechanisms through which data subjects may exercise their rights, among others.

[5] NPC Circular No. 2020-03, § 3.
[6] See: Data Privacy Act of 2012, § 4 (e), 12 (c) & (e) – for processing personal information, or 13 (b) & (f) – for processing sensitive personal information.
[7] NPC Circular No. 2020-03, § 8.

> The execution of a DSA is a sound recourse and demonstrates accountable personal data processing, as well as good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC. The Commission shall take this into account in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating thereto, as well as in the conduct of compliance checks."

Though the execution of a DSA is not mandatory, it is still advisable to execute a DSA as it is a best practice and a demonstration of accountability amongst the parties to the data sharing.

As to the parties to the same, only PICs can be parties to data sharing arrangements.[8] It may be possible for the DILG to represent the LCRs, where appropriate, subject to the applicable provisions of the Local Government Code of 1991 and/or DILG rules on the extent of the general supervision/jurisdiction of the DILG over cities and municipalities, including the LCRs.[9] The execution of DSAs is not intended to be onerous on the parties. Consider also that a DSA is not strictly in the form of a contract as the same may also be a joint issuance between or among government agencies.

Data sharing with the PSA

As to your second query on whether the execution of a DSA is required with the PSA for determining whether a pensioner is living or deceased, we reiterate that DSAs are optional. But for purposes of this particular sharing, we refer to a similar concern raised in relation to the updating of cancer registries as discussed in NPC Advisory Opinion No. 2018-054, to wit:[10]

> "In view of the foregoing, it is best to consult with the PSA Legal Service and clarify if it is possible for the DOH and the PCS to provide PSA with a list of specific individuals from their respective databases and for the latter to match this with its mortality database, i.e. provide a "Yes" or "No" answer as to the status of those individuals, taking into consideration the provisions of NPC Circulars No. 2016-01 (Security of Personal Data in Government Agencies) and 2016-02 (Data Sharing Agreements Involving Government Agencies)."

Also, since the proposed data sharing arrangement with the PSA has a similar purpose with that of the LCRs, PVAO may consider including the PSA as an additional party to the proposed DSA with the DILG. This, however, does not preclude your office from executing a separate DSA with the PSA should that be your preferred option.

For further details as to contents of a DSA, please refer to NPC Circular No. 2020-03 – Data Sharing Agreements available at https://www.privacy.gov.ph/memorandum-circulars/.

Government agencies as depositories of information; general data privacy principles

With respect to your third query, the LCR, PSA, and OTAG-NRD under the AFP, are separate PICs having their distinct mandates and purposes for processing personal data of their respective data subjects. PVAO is a third-party PIC with respect to the above.

[8] NPC Circular No. 2020-03, § 4.
[9] See: AN ACT PROVIDING FOR A LOCAL GOVERNMENT CODE OF 1991 [Local Government Code of 1991], Republic Act. No. 7160, § 25 and 479 (1991).
[10] National Privacy Commission, NPC Advisory Opinion No. 2018-054 (Dec. 4, 2018).

On whether information provided by data subjects to the aforesaid government agencies may be used and processed by the government in general, we take time to emphasize that the government is one of the biggest repositories of the personal data of citizens. The government or any its agencies, however, do not have the blanket authority to access or use the information about private individuals under the custody of another government agency.[11]

As discussed above, while government processing of personal data is recognized, the same is regulated by the provisions of the DPA. These agencies must process personal data for the fulfillment of a constitutional or statutory mandate, strictly adhere to all substantive and procedural processes involved in processing personal data, and observe the general data privacy principles of transparency, legitimate purpose, and proportionality.

Sharing within the offices under the DND

We are not privy as to the official organizational structure of the DND. Nevertheless, we understand that the AFP and the PVAO are attached agencies to the DND.[12] With this, they are considered as separate PICs and personal data shared between the two may be considered as data sharing.

The NPC is one with the PVAO and all government agencies in the fulfillment of their lawful mandates. As a regulator, we aim to implement the DPA to protect not only the rights of the data subjects but also to assist PICs in complying with their duties under the law.

These requirements are not meant to restrict the flow of information among government agencies since the DPA has the twin task of protecting the fundamental human right of privacy while ensuring the free flow of information to promote innovation and growth.[13] The DPA promotes fair, secure, and lawful processing of personal data.[14]

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

[11] National Privacy Commission, NPC Advisory Opinion No. 2018-007 (Feb. 26, 2018).
[12] Official Gazette, Department of National Defense, *available at* https://www.officialgazette.gov.ph/section/ briefing-room/department-of-national-defense/ (last accessed 7 March 2021).
[13] Data Privacy Act of 2012, § 2.
[14] See: National Privacy Commission, NPC Advisory Opinion No. 2018-083 (Nov. 26, 2018).