PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2025-001[1]

20 March 2025

[redacted]

Re: COMMISSION ON AUDIT'S ACCESS REQUEST TO THE DEPARTMENT OF AGRICULTURE'S DATABASE FOR AUDIT PREPARATION PURPOSES.

Dear [redacted]:

We respond to your request for an Advisory Opinion on the data privacy concerns relative to the sharing of information with the Commission on Audit (COA).

You state in your letter that the COA routinely requests the Department of Agriculture (DA) for the personal data of farmers and fisherfolk as part of its audit preparation process. In some instances, the COA also requests for access to the systems/database maintained by the Department of Agriculture - Information and Communications Technology Service (DA-ICTS) which contains the personal data of farmers and fisherfolks. The purpose of COA's request for access to the DA-ICTS is to verify the distribution of cash assistance to farmers. As legal basis for its access request, the COA cites COA Circular No. 2020-010,[2] underscoring the necessity for accurate and comprehensive audits.

Recently, the COA requested specific documents from the DA-ICTS containing the list of farmers from the Intervention Management Platform (IMP) who are eligible for discount vouchers or assistance through the Interventions Monitoring Card (IMC). The COA specifically instructed that the list must contain the full name, Registry System for Basic Sectors in Agriculture (RSBSA) Number, address, date of birth, and IMC Account Number of each farmer.

The DA granted the request lest it face a disallowance from the COA. Nevertheless, you seek guidance on the following:

[1] Tags: processing; personal data; mandate; audit function; security measures.
[2] Guidelines implementing COA Resolution No. 2020-034 relative to the Authority of COA Auditors to Access Information and Communications Systems, Electronic Data Messages and Source Documents of the Audited Entities Relevant to the Conduct of Audit.

1) Whether it is permissible to share the requested documents containing personal data with the Commission on Audit (COA) in the absence of a Data Sharing Agreement (DSA).

2) Whether the principle of proportionality under the Data Privacy Act of 2012 (DPA)[3] would be violated if the DA provides the COA with access to the database containing the personal data of farmers and fisherfolks.

Functions of public authority; constitutional or statutory mandate; Data Sharing Agreement.

Under Section 2, Article IX-D of the 1987 Constitution, the COA has the power, authority, and duty to examine, audit, and settle all accounts pertaining to the revenue and receipts of, and expenditures or uses of funds and property.

In Advisory Opinion No. 2020-016, we recognized the authority of the COA as an independent constitutional body and recognized its power, authority, and duty to examine, audit, and settle all accounts and expenditures of the funds and properties of the Philippine government. Thus, in carrying out its mandate, the COA enjoys the presumption of regularity in the performance of its duties.

The COA's request for the production of personal data of farmers and access to the DA-ICTS database containing the personal data of several individuals are considered as processing[4] under the DPA since it involves, among others, the collection, recording, or use of individual's personal data. Generally, the processing by public authorities pursuant to their respective mandate is considered lawful under Section 4(e) of the DPA.

Accordingly, the COA's request for personal data falls squarely within its constitutional mandate and is recognized under Section 4 (e) of the DPA. As such, the DA may lawfully share personal data of the farmers and fisherfolks with the COA.

The sharing of the individual farmer's data with the COA *sans* a Data Sharing Agreement is also permissible as Section 6 of NPC Circular 2020-03 (Data Sharing Agreements) does not prohibit nor limit the sharing, disclosure, or transfer of personal data which are already authorized or required by law. In the instant case, considering that the sharing, disclosure, or transfer of personal data is already authorized or required by law, the law or regulation itself may operate as the governing framework or protocol eliminating the need for a separate agreement. Thus, the execution of a DSA is discretionary, but compliance with the other provisions of the DPA, its Implementing Rules and Regulations (IRR), and relevant NPC issuances remains mandatory.

General data privacy principles; sensitive personal information Security measures;.

It must be stressed, however, that processing based on Section 4(e) of the DPA is not absolute. The IRR of the DPA clarifies that processing, even if pursuant to a legal mandate, must be

[3] Republic Act No. 10173.

[4] Processing refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

done lawfully and fairly, with strict adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality.

In particular, the principle of proportionality requires that personal information for processing must be accurate, relevant, adequate, and not excessive in relation to the specified and declared purpose. In addition, personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. As such, it is crucial to ensure that the information to be disclosed for audit purposes should only be limited to what is necessary to achieve the objectives of the audit.

In this regard, it is important to note that the RSBSA, IMC Account Number, and the date of birth of the individuals to be collected by the COA for audit purposes are classified as sensitive personal information (SPI) under Section 3(l) of the DPA. The RSBSA and IMC Account Number are unique identifiers issued by the DA peculiar to an individual while the date of birth can be used to ascertain an individual's age. In *Zoleta v. the Office of the Ombudsman*, the Supreme Court emphasized that an SPI, as compared to a non-sensitive or a non-privileged information, is more highly protected by laws due to its vulnerable nature. These types of personal information are subject to more stringent requirements before such could be lawfully processed.[5]

On this score, please note that even if the processing of SPI is allowed pursuant to existing laws and regulations there must be mechanisms in place on how the regulatory agency will guarantee the protection of the SPI. Chief Justice Gesmundo, in his concurring opinion in the *Philippine Stock Exchange v. Secretary of Finance*,[6] stated that the mere fact that the SPI is disclosed to a particular government agency only does not *ipso facto* guarantee that it will be secured absent any express guarantee that such data is safeguarded.

As such, as personal information controllers (PIC), the DA and the COA are also enjoined to conduct a Privacy Impact Assessment to determine the appropriate security measures to implement.[7] Likewise, PICs are required to regularly monitor for any security breaches and take preventive, corrective, and mitigating measures against incidents which may lead to security breaches. This is particularly significant as SPI are involved in the processing being undertaken.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished 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.

For your reference.

Very truly yours,

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

[5] Zoleta vs. Office of the Ombudsman, G.R. No. 258888, 08 April 2024.
[6] Philippine Stock Exchange v. Secretary of Finance, G.R. No. 213860, 05 July 2022, Concurring Opinion, C.J. Gesmundo.
[7] §4(d), NPC Circular No. 2023-06 (Security of Personal Data in the Government and Private Sector.