PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2024-001[1]

18 January 2024

[redacted]

Re: REQUEST FOR ACCESS TO PERSONAL DATA FOR AUDIT PURPOSES

Dear [redacted]:

We respond to your request for an Advisory Opinion regarding the Commission on Audit's (COA) request to access personal and sensitive personal information in relation to its performance audit.

You mention that the COA is conducting a performance audit on the COVID-19 National Vaccination Program, which is helmed by the Department of Health (DOH). As part of the audit process, the COA's audit team needs access to the COVID-19 Vaccination Information Management System (VIMS) to review the accuracy and reliability of data generated therefrom. The Epidemiology Bureau (EB) of the DOH maintains processing over the VIMS and serves as the primary source of information for the nationwide vaccination status posted on the DOH website.

However, the DOH expressed concerns about data privacy regarding the COA's request for access to the VIMS. The DOH reasoned that the local government units (LGUs) were solely responsible for collecting the data stored in the VIMS, while EB's role is limited to storing and managing the data in accordance with its mandate. Although the audit team had already conducted tests of the data against the source documents held by the LGUs, the conduct of a national-level review of the data from the VIMS will achieve a different audit objective.

You thus seek guidance on how to conduct the audit process in compliance with the Data Privacy Act of 2012 (DPA).

[1] Tags: processing; audit function; constitutional mandate.

NPC Advisory Opinion No. 2020-016; constitutional or statutory mandate.

We reiterate our stance in NPC Advisory Opinion No. 2020-016 in which we acknowledged 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.[2] We also stated therein that:

> The DPA shall not be used to hamper, or interfere with, the performance of the duties and functions of duly constituted public authorities. Pursuant to the 1987 Constitution, the COA shall have exclusive authority, subject to certain limitations, to define the scope of its audit and examination, establish the techniques and methods required therefor, and promulgate accounting and auditing rules and regulations, including those for the prevention and disallowance of irregular, unnecessary, excessive, extravagant, or unconscionable expenditures or uses of government funds and properties.
>
> With this in mind, the COA in carrying out its mandate, enjoys the presumption of regularity in the performance of its duties. The determination of what methods to utilize in the collection or gathering of personal data in performing its auditing functions shall be left to the COA's sound discretion.

As such, the COA's intended access to the VIMS database to review its completeness, reliability, and overall performance falls within COA's constitutional mandate and, hence, the processing thereof is generally allowed.[3]

General data privacy principles; Security measures

Please note that although the COA has the authority to process personal data pursuant to its mandate, it still bears the responsibility of following other rules and regulations laid out in the DPA, its IRR, and any other guidelines set by the National Privacy Commission (NPC). This means that COA must process personal data lawfully and fairly, with strict adherence to the general data privacy principles. It is important to note that personal data collected must be proportionate, adequate and not excessive in relation to the original purposes for which they were collected,[4] which is particularly relevant in the given scenario.

The COA is also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the processed personal data. Furthermore, it is also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[5] This is particularly significant as the data being processed are classified as sensitive personal information. Additionally, COA must ensure that the audit is confined only to data related to the COVID-19 National Vaccination Program, as specified in the engagement letter addressed to the DOH.

[2] § 2(1), Article IX-D, The 1987 Philippine Constitution.
[3] § 4(e), Data Privacy Act of 2012.
[4] § 11(d), Data Privacy Act of 2012.
[5] § 20 (c) (4), Data Privacy Act of 2012.

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