



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2020-016¹

12 March 2020



Re: **AUDIT PROCEDURES OF THE COMMISSION ON AUDIT**

Dear 

We write in response to your request for an advisory opinion seeking guidance vis-à-vis the Commission on Audit (COA) Memorandum which states that the Data Privacy Act of 2012² (DPA) does not absolutely prohibit access to information since the law itself has exceptions, and that auditees cannot validly deny the COA access to information/details based on the DPA.

In your letter, you stated that although you acknowledge the functions of the COA, pursuant to its constitutional mandate to examine, audit, and settle all accounts pertaining to the revenue, receipts, and expenditures or uses of funds and property owned or held in trust by, or pertaining to, the government,³ you have reservations regarding the manner to be employed by COA in the acquisition of personal information, specifically if the same will be done through remote access or database cloning which may pose risks and may lead to personal data breach.

Public authority; constitutional or statutory mandate

The COA is a constitutional commission, created precisely to be one of the pillars of the State's system of checks and balances. As a public authority, it has the mission to ensure accountability for public resources, promote transparency, and help improve government operations, in partnership with stakeholders, for the benefit of the Filipino people.⁴

¹ Tags: COA; processing of public authorities; constitutional or statutory mandate; presumption of regularity; 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, § 4 (e) (2012).

³ Phil. Const. art. IX § 2 ¶ D.

⁴ Commission on Audit website, Commission on Audit Mission, available at https://www.coa.gov.ph/coa_at_a_glance/index.html#mission (last accessed 11 March 2020).

We must be reminded that the processing of information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, subject to restrictions provided by law, is one of the instances where the application of the Data Privacy Act of 2012⁵ (DPA), and of the DPA's Implementing Rules and Regulations⁶ (IRR), is qualified or limited.

This means that when the personal information is needed to be processed by a public authority, such as the COA, pursuant to its constitutional mandate, the processing of such personal data is generally allowed by the aforementioned enactments.

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.⁷

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.

The Supreme Court, in the case of *Yap v. Lagtapon*, held that "the presumption of regularity in the performance of official duties is an aid to the effective and unhampered administration of government functions. Without such benefit, every official action could be negated with minimal effort from litigants, irrespective of merit or sufficiency of evidence to support such challenge. To this end, our body of jurisprudence has been consistent in requiring nothing short of clear and convincing evidence to the contrary to overthrow such presumption."⁸

Applying such ruling in this case, absent any proof that the methods adopted by the COA in gathering personal data may be violative of the provisions of the DPA, the presumption of regularity in the carrying out of its official duties stands.

General data privacy principles; proportionality; obligations of personal information controllers

On the other hand, the foregoing does not relieve the COA, as a personal information controller (PIC), of its duties as such under the DPA. The constitutional provision allowing the COA to determine the scope, method and extent of auditing, including the gathering of personal data from its auditees, shall not be construed to have waived the application of the DPA.

⁵ 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, § 4 (e) (2012).

⁶ Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) (2016).

⁷ PHIL. CONST. art. IX-D § 2.

⁸ *Yap v. Lagtapon*, 803 PHIL 652, (2017).

As your office correctly pointed out, the COA must still abide by the general data privacy principles provided under the DPA and its IRR, particularly the principle of proportionality. This means that in the processing of personal data, the COA must see to it that the personal data collected and processed shall be adequate, relevant, suitable, necessary, and not excessive in relation to its declared and specified purpose, and that personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.⁹ Thus, the methods to be used in conducting audits may be further assessed if the same are proportional methods vis-à-vis the purposes as well as risks these may pose.

Nonetheless, we trust that the COA, as a PIC, is aware of its obligations under the DPA, its IRR, and issuances of the NPC, specifically NPC Circular No. 16-01 on the Security of Personal Data in Government Agencies, which includes the implementation of physical, organizational and technical security measures for the protection of personal data, among others, and NPC Circular No. 16-03 on Personal Data Breach Management.

This opinion is rendered based on the information you have provided. Additional information may change the context of the inquiry and the appreciation of the facts.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

⁹ Rules and Regulations Implementing the Data Privacy Act of 2012, § 18 (c).