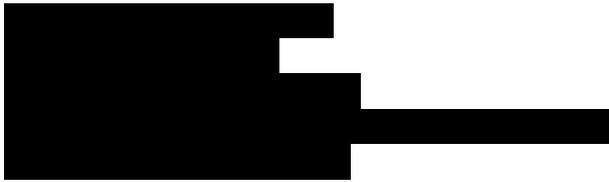




Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-002**

15 January 2018



**Re: COMMISSION ON AUDIT (COA) REQUEST FOR ACCESS
TO BANGKO SENTRAL NG PILIPINAS (BSP) EMPLOYEES'
DIRECTORY**

Dear ,

This is with regard to your query received by the National Privacy Commission (NPC) on 21 November 2017 on the request of the Commission on Audit (COA) for access to the directory of employees posted in the BSP intranet vis-a vis COA's position that it is exempt from the application of Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA) in the performance of its constitutionally-mandated auditing functions.

We understand that the BSP employee directory contains the following information:

1. Employee name;
2. Position;
3. Office;
4. Office contact numbers;
5. E-mail address; and
6. Photograph.

Scope

Section 4 of the DPA states that the law is applicable to the processing of all types of personal information and to any natural and juridical person involved in personal information processing, including those personal information controllers and processors, who, although not found or established in the Philippines, use equipment that are located in the Philippines or who maintain an office, branch or agency in the Philippines.

Section 4(a) and (e) states some of the special cases where the law does not apply, to wit:

“(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

- (1) The fact that the individual is or was an officer or employee of the government institution;
- (2) The title, business address and office telephone number of the individual;
- (3) The classification, salary range and responsibilities of the position held by the individual; and
- (4) The name of the individual on a document prepared by the individual in the course of employment with the government.

xxx xxx xxx

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions. xxx.”

Special Cases

In excluding from its scope these categories of information, it does not similarly exclude personal information controllers or personal information processors. Thus, even if a particular information does not fall within the scope of the DPA, this is not a blanket exemption and neither does this exemption extend to the natural or juridical person involved in the personal data processing.

We reiterate that the exemption is not an exemption on the entity or agency but on the type of information processed. This is interpreted to the effect that there is a presumption that personal data may be lawfully processed by a personal information controller or processor under the special cases provided above, but the processing shall be limited to achieving the specific purpose, function or activity, and that the personal information controller or processor remains to be subject to the requirements of implementing measures to secure and protect personal data.

For instance, a government agency having a constitutional or statutory mandate to collect and process personal data may do so even without the consent of the data subject. But this is with the concomitant responsibility of ensuring that organizational, physical and technical security measures are in place to protect the personal data it is processing.

The exemption particularly pertains to information on any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual information, and information which is necessary in carrying out the functions of a public authority, in accordance to its law enforcement and regulatory mandate under the Constitution or law creating it.

Being an exception to the rule, it must be established that the information claimed to be outside the scope of the DPA is:

1. About a current or former government employee/officer which relates to his or her position or functions; or

2. Necessary in order to carry out the functions of public authority, and processing of personal data is for the performance of a constitutional or statutory mandate.

Thus, only the information required to be processed pursuant to the said function shall not be covered by the law to the minimum extent necessary, while COA, as an entity, is still covered by the DPA.

This means that the COA, as a personal information controller, is mandated under the DPA to adhere to the data privacy principles of transparency, legitimate purpose and proportionality.

In determining whether the personal data being collected by the COA is necessary to carry out its functions, the personal data would have to be processed pursuant to a legitimate purpose, and in a proportional and transparent manner. COA must also implement appropriate security measures for personal data protection, and ensure that data subjects are able to exercise their rights within the limits provided by law.

Thus, if COA's processing of personal information, i.e. access to BSP's employee directory, is not necessary to its constitutionally mandated functions, such processing should therefore be anchored on any of the criteria for lawful processing as stated in Section 12 and Section 13 of the DPA for personal and sensitive personal information, respectively.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman