



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-61**

03 October 2017



**Re: COMPLIANCE WITH THE NATIONAL PRIVACY
COMMISSION REQUIREMENTS**

Dear 

This refers to your query which was received by the National Privacy Commission (NPC) on 9 August 2017. Specifically, you put forward the following inquiries:

1. What are the requirements of the NPC to be submitted on/or before 9 September 2017?
2. Can the Human Resource Department (HRD) disclose information particularly about the health of your former employee to the latter's prospective employer?
3. Can the Legal Department provide alternative means instead of a) providing personal information collection statements to employees and clients, and b) drafting data sharing agreements and non-disclosure agreements?

Registration of Data Processing Systems

Section 47 of the Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012 (DPA) in relation to Section 5 of NPC Circular No. 17-01 requires the registration of the data processing systems of personal information controllers (PICs) and personal information processors (PIPs) under the following conditions:

- A. the PIC or PIP employs at least two hundred fifty (250) employees;
- B. the processing includes sensitive personal information of at least one thousand (1,000) individuals;
- C. the processing is likely to pose a risk to the rights and freedoms of data subjects.

- D. the processing is not occasional: *Provided*, that processing shall be considered occasional if it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional

The registration process is in two (2) phases. Phase 1 requires the information on the designation of the PIC's Data Protection Officer (DPO) through an application form and supporting documents:

A. For government agencies:

1. certified true copy of the Special/Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP; and
2. where applicable, a copy of the charter of the government entity, or any similar document identifying its mandate, powers, and/or functions.

B. For private entities:

1. duly-notarized Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation.
2. certified true copy of the following documents, where applicable:
 - a. General Information Sheet or any similar document;
 - b. Certificate of Registration (SEC Certificate, DTI Certification of Business Name or Sole Proprietorship) or any similar document; and/or
 - c. Franchise, license to operate, or any similar document.

Currently, registration requires manual submission of the hard copy application form to NPC at Core G, 3/F GSIS Headquarters, Financial Center, Pasay City. The deadline is on 9 September 2017.

Phase 2 shall be through an online registration platform, whereby the details of the data processing system or systems shall be required, among others. The deadline for Phase 2 is on 8 March 2018.

Lawful Processing of Personal Data - Disclosure

According to the DPA, the term "processing" refers any operation performed upon the personal data including, but not limited to, collection, access, disclosure of data.¹

The processing of health data, which is sensitive personal information, of a former employee is PROHIBITED, except for any of the following cases:²

- The data subject has given his or her consent, specific to the purpose to the processing;

¹ RA No. 10173, §3

² Id., §13

- The processing, use is done as mandated by existing laws and regulations;
- The processing is necessary to protect the life and health of the patient or another, and the owner of the cellular phone is not legally or physical able to express his or her consent prior to the processing;
- The processing is necessary to achieve lawful and noncommercial objectives of public organizations and associations;
- The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; and
- The processing concerns sensitive personal information or privileged information necessary for the protection of lawful rights and interest of natural or legal personal in court proceedings, or the establishment, exercise, or defense of legal claims, or when provided to government or public authority pursuant to a constitutional or statutory mandate.

Thus, the HRD should consider the foregoing prior to disclosing any health information of the former employee.

Further, in consideration of the rights of the data subject under the DPA, the former employee should be informed of the extent of disclosure of his or her health information.³ The disclosure of any information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.⁴

Mandate of Tourism Information Enterprise Zone Authority (TIEZA)

Based on the limited information, any alternatives to privacy notices, data sharing agreements and non-disclosure agreements, would have to be evaluated based on the nature of processing concerned, what data is involved and the purpose of processing. The PIC may forego obtaining consent in the processing of personal data, only if there is a constitutional or statutory basis for the processing where consent is not required. This may require documenting the basis of the processing in relation to the mandate of the agency and any other existing law or regulation.

Data Sharing Agreement and Non-Disclosure Agreement

With regard to the data sharing agreements (DSAs) and non-disclosure agreements (NDAs), DSAs are required when there is sharing of personal data between government agencies for the purpose of a public function or provision of a public service.⁵

Note that a DSA may take the form of a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement.⁶ If there is already an existing written documentation on the sharing agreement, there is a need to review the same and determine compliance with the IRR and NPC Circular No. 16-02.⁷

³ IRR of RA 10173, §18(a)

⁴ *Id.*, §18(b)

⁵ *Id.*, §20(d)

⁶ NPC Circular No. 16-02, §3(E)

⁷ NPC Circular No. 16-02, §19

On the other hand, there is no explicit requirement under the DPA, IRR and issuances of the NPC on the need for an NDA. But where personal data is required to be kept confidential, one contractual way to ensure the same is through the execution of NDAs.

For your reference.

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman