Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017- 44

16 August 2017

[redacted]

Re: REQUEST FOR OPINION ON EXEMPTION FROM THE REGISTRATION REQUIREMENT WITH THE NATIONAL PRIVACY COMMISSION

Dear [redacted],

This pertains to your request for advisory opinion which sought to clarify the following matters regarding Republic Act No. 10173[1], also known as the Data Privacy Act of 2012 (DPA):

1. Whether APO Production Unit, Inc. (APO) is required to register with the NPC;
2. Whether the potential third party supplier and its subsidiaries are required to register with the NPC, and whether the potential supplier's regional compliance officer is sufficient compliance with the DPA.
3. How business processes abroad (e.g. cross border data processing and transfer of data to affiliates abroad) are affected by the DPA;
4. Whether entities based abroad that process information from the Philippines are subject to the registration requirements of the DPA; and
5. Penalties imposable for failure to register.

In your letter-request, you have narrated that APO is a government instrumentality with corporate powers, and is a recognized government printer. APO was engaged by the Department of Foreign Affairs (DFA) to produce, deliver and manage the e-Passport system. Due to this engagement, APO collects, organizes, uses and stores personal data of e-Passport applicants, as well as the actual printing of the e-Passports.

[1] AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIACY COMMISSION, AND FOR OTHER PURPOSES, "Data Privacy Act of 2012" (15 August 2012).

It is indeed accurate to state that the DPA primarily deals with personal information controllers[2] (PICs) and personal information processors[3] (PIPs) who process personal information and sensitive personal information of data subjects. Based on the definitions provided by law, APO may be considered as a PIP who is directed or instructed by the PIC, the DFA in this case, to process personal information according to the objectives of the e-Passport Project.

APO is not allowed to process personal information of the e-Passport applicants, outside the provisions of its contract with the DFA or for its own purpose. In addition, APO may also be considered as a PIC, relative to its own operations as a production unit, as a corporate entity.

However, it must be clarified that the issuance of e-Passports by the DFA pursuant to its mandate excludes such information from the coverage of the DPA. Section 4 of the law and Section 5 of the Implementing Rules and Regulations (IRR) exempt specific types or classes of information from its scope - in particular, paragraph (e) of the latter states:

> "Section 5. Special Cases. ***The Act and these Rules shall not apply to the following specified information,*** only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:
>
> xxx xxx xxx
>
> e. ***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,*** including the performance of the functions of the independent, central monetary authority, subject to restrictions provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act, Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
>
> xxx xxx xxx
>
> Provided, that ***the non-applicability of the Act or these Rules do not extend to personal information controllers or personal information processors***, who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be ***exempted from the***

---

[2] *Id*., §3(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose perosnal information on his or her behalf. This term excludes: (1) A person or oganization who performs such functions as instructed by another person or organization; and (2) An individual who collects, holds, processes or use personal information in connection with the individual's personal, family or household affairs.

[3] *Id*., §3(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

***requirements of the Act only to the minimum extent necessary to achieve the specific purpose, function, or activity.*"** (Emphasis supplied).

From the provision above, it is evident that the non-applicability of the law will only apply to the minimum extent of collection, access, use, disclosure or other processing activities. However, the non-applicability does not extend to the duties and responsibilities of the entity or organization as a PIC or PIP, such as the duty to uphold the rights of data subjects, to designate a Data Protection Officer, to ensure implementation of security measures to protect personal data, among others.

Hence, the DFA is only exempt to the minimum extent of such processing activities. Also, the limited exemption granted to the DFA does not extend to APO because the law treats each entity or organization individually.

Given the resolution above, APO, as both a PIC and a PIP is obliged to comply with the provisions of the DPA, its IRR and other NPC issuances applicable to its processing activities. Chief among these obligations is the adherence to the general data privacy principles of transparency, legitimate purpose, and proportionality. Another requirement is the need to appoint a data protection officer (DPO).

Pursuant to Section 21(b) of the DPA and Section 50(b) of the IRR, PICs shall designate an individual or individuals who are accountable for the organization's compliance with this Act. This is further elucidated under NPC Advisory No. 2017-01 dated 14 March 2017.

APO is likewise required to implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.[4]

Registration of APO with the NPC

Section 47 of the IRR provides for the registration of personal data processing systems. PIC or PIP shall register their Data Processing Systems under the following circumstances:

1. When the personnel employed are <u>at least</u> two hundred fifty (250) persons;
2. The processing includes sensitive personal information of at least one thousand (1,000) individuals;
3. The processing it carries out is likely to pose a risk to the rights and freedoms of the data subjects; or
4. The processing is not occasional.

In case any of the circumstances enumerated above are present, APO is then required to register its data processing system.

Please refer to NPC Circular No. 2017-01 - Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making for additional details on the registration process.

---

[4] *Id.*, §20.

Registration of the third party supplier and its subsidiaries with the NPC

You have mentioned in your letter-request that you have a potential supplier with two (2) subsidiaries in the Philippines. The first one has more than two hundred fifty (250) employees and collects personal and sensitive personal information. Following the criteria discussed above, indeed, the first one must register with the NPC.

As to the second subsidiary, although there are less than two hundred fifty (250) employees, but if it processes sensitive personal information of at least one thousand (1,000) individuals, registration is required.

In addition, given that these entities are covered by the DPA, they are mandated to designate a DPO. If the regional compliance officer of the said supplier can sufficiently perform the duties and responsibilities of a DPO and possess the qualifications enumerated in NPC Advisory No. 2017-01[5], then, the regional compliance officer can be the designated DPO.

Effect of the DPA to businesses abroad

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing in the Philippines,[6] and has extraterritorial application in certain instances, i.e. an act done or practice engaged in and outside of the Philippines by an entity if the act, practice or processing relates to personal information about a Philippine citizen or a resident, etc.[7]

With this, it is possible that the DPA will be applicable to processing done abroad as provided in Section 6 of the DPA, and other relevant sections of the IRR on data sharing and outsourcing will likewise be applicable.

However, for the registration requirement, Section 46(a) of the IRR provides that "pursuant to the mandate of the Commission to administer and implement the Act, and to ensure the compliance of personal information controllers with its obligations under the law, the Commission requires the registration of personal data processing systems operating in the country…"

This is interpreted to mean that only those personal data processing systems physically operating in the Philippines would be covered by the registration requirement.

Penalties imposable for violations and non-compliance with the provisions of the DPA, its IRR and other NPC issuances

As a general rule, processing of personal data must be authorized under the Data Privacy Act and existing laws. This means that a personal information controller or personal information processor must be able to demonstrate compliance with the law, its IRR and

[5] NPC Advisory No. 2017-01: Designation of Data Protection Officers (14 March 2017).
[6] Supra note 1
[7] Id., §6

related issuance, including requirements for designation of a DPO, registration of data processing systems and notification of automated decision-making.

A PIC or PIP whose certificate of registration has been revoked or that is determined to have violated the registration requirements may, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent bans on the processing of personal data, or payment of fines in accordance with a schedule to be issued by the Commission.

Failure to comply with an order of the Commission, may in addition, subject the PIC or PIP to contempt proceedings filed in the proper court. In case of the occurrence of a personal data breach, the filing of a complaint by a data subject, or a privacy compliance check of the National Privacy Commission, the failure of the PIC or PIP to comply with the law, IRR and issuances shall be considered when determining exercise of due diligence of the PIC or PIP and liability.[8] These may be duly meted out by the NPC should the circumstances warrant the same.

For your reference.

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[8] *Supra* note 1, §25-33