Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-012[1]

17 January 2019

[redacted]

Re: NATIONALITY OF DATABASE HOST

Dear [redacted],

We write in response to your letter to the National Privacy Commission (NPC) requesting for guidance on the database utilized by the Firearms and Explosives Office (FEO).

Based on your letter, the FEO already processes online the applications for License to Own and Possess Firearm (LTOPF) and Firearm Registration for individuals and juridical entities. Currently, the FEO database for said application and registration is hosted by a foreign entity. You now seek clarity on the following questions:

1) Is there a legal impediment when the database is hosted by a foreign entity?
2) Is there a requirement in the law that government databases should be hosted only by a Filipino owned company?
3) Should the FEO opt to change the hosting of its databases to a Filipino owned company, is there a clearance requirement from the NPC?

No legal impediment for foreign host of database

The Data Privacy Act of 2012[2] (DPA) does not prohibit hosting of government databases by a foreign entity. There is no requirement in the DPA relating to the nationality of service providers, either for the government or the private sector. In cases where a personal information controller[3] (PIC) subcontracts or outsources the processing of personal data to a personal information processor[4](PIP), such as the engagement of a service provider for hosting services, the PIC remains primarily accountable for the protection of personal data

[1] Tags: Government database, nationality requirement
[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 (2012).
[3] Data Privacy Act of 2012, § 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 personal information on his or her behalf. xxx.
[4] *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.

under its control, even when it is already being processed by a PIP. Thus, the FEO is required to "use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes."[5] The FEO must also consider the provisions on outsourcing or subcontracting of personal data processing under the law and its Implementing Rules and Regulations[6] (IRR), and relevant provisions in Circular 16-01, "Security of Personal Data in Government Agencies" (2016) [7]

Considerations in the engagement of a database host

With respect to the obligations of the foreign database host as a PIP, the FEO may consider the following elements of the subcontracting or outsourcing contract as indicated in Section 44 of the IRR:

a. The contract or legal act shall set out ***the subject-matter and duration*** of the processing, the ***nature and purpose*** of the processing, ***the type of personal data and categories of data subjects***, the ***obligations and rights*** of the personal information controller, and the ***geographic location*** of the processing under the subcontracting agreement.

b. The contract or other legal act shall stipulate, in particular, that the personal information processor shall:

    1. ***Process the personal data only upon the documented instructions of the personal information controller***, including transfers of personal data to another country or an international organization, unless such transfer is authorized by law;
    2. ***Ensure that an obligation of confidentiality is imposed on persons authorized*** to process the personal data;
    3. ***Implement appropriate security measures*** and comply with the Act, these Rules, and other issuances of the Commission;
    4. ***Not engage another processor without prior instruction*** from the personal information controller: Provided, that any such arrangement shall ensure that the same obligations for data protection under the contract or legal act are implemented, taking into account the nature of the processing;
    5. Assist the personal information controller, by appropriate technical and organizational measures and to the extent possible, fulfill the obligation to respond to requests by data subjects relative to the exercise of their rights;
    6. Assist the personal information controller in ensuring compliance with the Act, these Rules, other relevant laws, and other issuances of the Commission, taking into account the nature of processing and the information available to the personal information processor;
    7. ***At the choice of the personal information controller, delete or return all personal data to the personal information controller after the end of the provision of services*** relating to the processing: Provided, that this includes deleting existing copies unless storage is authorized by the Act or another law;
    8. Make available to the personal information controller all information necessary to demonstrate compliance with the obligations laid down in the Act, and ***allow for and contribute to audits, including inspections***, conducted by the personal information controller or another auditor mandated by the latter;
    9. Immediately inform the personal information controller if, in its opinion, an instruction infringes the Act, these Rules, or any other issuance of the Commission.

[5] Rules and Regulations Implementing the Data Privacy Act of 2012, § 43.
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
[7] NPC Circular 16-01, Security of Personal Data in Government Agencies, Rule II, § 7 (2016). *See also* §§ 8-13.

As a government entity, the FEO should also look at NPC Circular No. 16-01 on Security of Personal Data in Government Agencies for guidance on standards relating to data protection. Additionally, there are industry standards which the FEO should consider in determining the adequacy of their database host, such as the following:

a) ISO 27002 (Code of Practice for Information Security Controls) – this provides for general security controls, including databases;
b) ISO/IEC 27040 (Storage Security) – considering that databases are a form of data at rest; and
c) ISO 27018 (Code of Practice for Protection of Personal Identifiable Information "PII" Protection in Public Clouds acting as PII Processors) and ISO 9579 (Remote Database Access with Security Enhancement) – considering that the government is promoting a Cloud First Policy and the FEO is already using cloud computing for their databases.

No clearance requirement needed from the NPC for change of host

Lastly, in case the FEO opts to change the provider or host of its databases to a Filipino owned company, there is no clearance requirement from the NPC. However, the FEO must ensure that the previous host complies with its contractual obligations, significantly those relating to access, retention or deletion of data. The NPC reserves the right to audit a government agency's data center or that of its service provider. NPC may also require the agency to submit its contract with its service provider for review.[8]

Accountability is one of the key principles of data protection under the Data Privacy Act. Government agencies are responsible for personal data under its control, including information that have been transferred to a third-party for processing, whether domestically or internationally. The government agency, as a PIC, must be able to demonstrate that it has ensured a comparable level of protection, consistent with the DPA and other issuances, while personal data is being processed on its behalf by third parties.

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

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

Noted by:

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[8] NPC Circular 16-01, Security of Personal Data in Government Agencies, Rule II, § 7 (2016). *See also* §§ 8-13.