Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2019-004[1]

4 January 2018

[redacted]

Re: DATA SHARING ARRANGEMENTS WITH OFFSHORE COMPANIES

Dear [redacted],

We write in response to your request for guidance on data-sharing arrangements entered into by PLDT with entities outside of the Philippines.

We understand that PLDT frequently enters into agreements with offshore companies to be able to provide products and services to its clients. These offshore companies either act as a personal information controller (PIC) or a personal information processor (PIP) depending upon the nature of service that they provide and the purpose of engagement.

We understand further that contractual discussions on compliance with the Data Privacy Act of 2012 (DPA)[2] have been a challenge for PLDT as these offshore companies may be unwilling to agree to data privacy commitments. Hence, you ask for guidance on possible courses of action or any framework that has been agreed upon by data privacy authorities to address the matter.

Scope of the DPA; contractual agreements involved

The DPA applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing.

An entity may either be a PIC who controls the collection, holding, processing or use of personal data or instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, or it may be a PIP to whom a PIC may outsource the processing of personal data, whereby it is directed by the PIC to perform any of the processing activities in accordance with its instructions.

---

[1] Tags: data sharing, outsourcing, personal information controller, personal information processor, compliance

[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).

Where an offshore company acts as a PIC with its own purpose of processing, completely separate from the declared purpose of PLDT, a data sharing agreement is required.

On the other hand, where an offshore company acts as a PIP, contracted by PLDT to perform particular processing activities on its behalf, the outsourcing or sub-contracting agreement shall reflect the security measures involved in processing, including the transfer of data, use, storage and retention.

Data sharing and compliance with the DPA

All PICs and PIPs are mandated to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and issuances of the National Privacy Commission (NPC).

PICs that share personal data under a data sharing agreement are mandated to put in place adequate safeguards for data privacy and security in compliance with applicable laws and regulations. The DSA should include a general description of the security measures that will ensure the protection of the personal data of data subjects. The DSA, considering its terms, allows PICs to use contractual and reasonable means to provide safeguards for data protection to the personal data being shared.

Where a PIC fails to put in place the security measures required by law, regulations and the DSA, the said PIC may be solely accountable in the absence of fault or negligence on the other PIC. If no security measures are put in place by both parties or the DSA fails to provide for the same, both parties may be held accountable. Nonetheless, the determination of liability, if any, will be based on the particular facts and circumstances of the case.

For data sharing between PLDT and another PIC, Section 20 of the IRR of the DPA should be followed and NPC Circular No. 16-02[3] may be referred to for guidance.

Duty of the PIC to ensure that the PIPs comply with the DPA

It is recognized under the DPA that PICs may enter into agreements with other entities to process personal data on their behalf. Section 14 of the DPA states:

> "SECTION 14. Subcontract of Personal Information. —A PIC may subcontract the processing of personal information, provided, that the PIC shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws."

In addition, Section 21 on accountability states as follows:

> "SECTION 21. Principle of Accountability. — Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

[3] National Privacy Commission, Data Sharing Agreements Involving Government Agencies Circular No. 16-02 [NPC Circular 16-02] (10 October 2016).

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party."

As can be gleaned from the provisions above, it is the ultimate responsibility of the PIC to engage PIPs that are compliant with all applicable laws. The PIC is duty-bound to place the pertinent data privacy and protection provisions in the contract. The agreement with the PIP must comply with Section 44 of the IRR of the DPA, to wit:

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 implement, 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 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.

Failure to comply with the provisions of the DPA and the IRR on outsourcing agreements will be duly considered by the NPC in case there is a compliance check, personal data breach, complaint, or an investigation, among others. This may result into findings where both the PIC, PLDT in this case, and the PIP, are liable for any of the punishable acts under the DPA.

As a PIC, PLDT has control over which entities to engage and contract with and it has the prerogative to continue the contractual relationship. It must determine internally if continuing contracts with non-compliant entities is viable for the business, taking into consideration the

attendant risks of such relationship vis-à-vis the requirements of the DPA and the expectations of its data subjects.

This opinion is based solely on the limited 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