Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-057

20 September 2018

[redacted]

Re: OUTSOURCING AGREEMENT

Dear [redacted],

We write in response to your query received by the National Privacy Commission (NPC) via email. You stated that Automatic Data Processing (ADP) is a human capital management solutions company based in the United States. It has presence in the Philippines through ADP (Philippines) Inc. which provides payroll services to Philippine clients. You seek advice and clarification regarding Section 44 of the Implementing Rules and Regulations (IRR)[1] of Republic Act No. 10173,[2] otherwise known as the Data Privacy Act of 2012 (DPA).

We provide the following clarifications:

1. On Section 44 of the IRR, you inquire if there are any restrictions on modifying the terms used in the same provision for data outsourcing agreements.

We confirm that Section 44 of the IRR on Agreements for Outsourcing does not prevent the parties to the contract from modifying the same if the required stipulations laid down in Section 44(b) are clearly set out therein. The parties may add or provide other terms and conditions in the outsourcing agreement.

2. On Section 44 (a), particularly on the requirement to indicate the geographical location of processing in relation to your multinational clients with a global presence which require multiple data hosting locations, you seek advice on whether your current approach, i.e. providing clients with an indicative list of countries where their data will be hosted and accessed, obtaining a blanket approval for cross border data transfers in the contract and communicate changes, if any, on a set frequency, either annually, bi-annually or quarterly, meets the requirement under the law.

[1] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
[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).

It is sufficient that the agreement states the indicative list of countries where personal data of clients that require multiple data hosting locations will be processed. We further note that in case there may be changes, the same should be communicated to the parties to the contract. In the case of cross-border data transfers, the applicable laws of the different jurisdictions and international agreements, if any, will apply.

The DPA provides for no restrictions on cross-border data transfers from a personal information controller to a personal information processor located in another jurisdiction so long as the PIC ensures that proper safeguards are in place to ensure the confidentiality, integrity and availability of the personal data processed, and prevent its use for unauthorized purposes as well as comply with the requirements of the DPA, the IRR and other issuances of the Commission.

3. On Section 44 (b)(1) and (4) on the processing by another processor or sub-contractor, you inquired whether including a blanket approval in the contract for (a) cross border data transfers and (b) engaging another processor/sub-contractor/vendor, subject to the same confidentiality, security and privacy provisions, meet the requirement of the IRR? Would proactively communicating cross-border data transfers/processor changes to clients prior to implementing said changes and providing a mechanism to object to the change satisfy the requirement in IRR?

The personal information controller should already be apprised of the possible jurisdictions where personal data will be transferred to as well as the possible engagement of another processor, sub-contractor or vendor if the same can be already identified. The proposed communication of changes on cross-border transfers/processors or sub-contractors should, at the very least, provide a mechanism that gives the personal information controller a sufficient period of time to object before the proposed changes are implemented in order to comply with the requirements of the IRR. As mentioned above, kindly note that stipulations on cross-border data transfers are always subject to the laws and regulations of the particular jurisdictions involved.

4. On Section 44 (b)(7) on retention of data, you stated that from a technology standpoint, data on archival media/backup tapes cannot be disturbed or destroyed. You seek clarification on whether archives and backup tapes may be exempt from the requirement under the DPA for the deletion of existing copies.

No, archival media or backup tapes are not exempt from the law. While personal data may be retained for a certain period pursuant to legitimate business purposes, such purpose must be consistent with standards followed by the applicable industry.[3] Taking into consideration the technical challenges, companies must start considering strategies on how to make data erasure possible, or how to put in place measures to prevent further processing of data on archival media/backup tapes. The DPA provides that personal data shall not be retained longer than necessary.[4] Where data is being retained, PICs should document its justification and ensure that data subjects are fully notified of such retention, the purpose and other relevant information.

5. On Section 44 (b)(8) on the requirement to make available to the personal information controller all information necessary to allow for and contribute to audits by said PIC or

[3] Id., § 19 (d)(1)(c).
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, § 19 (d).

another auditor mandated by the PIC, you inquire whether there is further guidance on said provision; whether it is possible to restrict such an audit to select situations which require an audit and establish terms and conditions that would require the audit to be performed in a manner that would not compromise another client's data or the vendor's internal protocols; and whether it is possible to require the parties to mutually agree on the auditor.

The purpose of the provision is to allow the personal information controller to have access to necessary information in the hands of the processor in case of audits and inspections. The audits and inspections contemplated in the provision are not limited to those conducted by the personal information controller itself or another auditor mandated by the latter, but also those required by the DPA, its IRR and pertinent issuances of the NPC.

The parties may include appropriate stipulations on the conduct of audit in certain circumstances, as well as those which would require audits to be performed in a manner that would not compromise another client's data or the PIP's internal protocols, and even the requirement that parties shall mutually agree on the auditor, if feasible.

All of these are subject to the precept that contracting parties may establish such stipulations, clauses, terms and conditions as they may deem convenient, provided they are not contrary to law, morals, good customs, public order, or public policy.[5]

This opinion is being rendered based on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of the 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

[5] An Act To Ordain And Institute The Civil Code Of The Philippines [THE CIVIL CODE OF THE PHILIPPINES] Republic Act. No. 386 (1949), Art. 1306.