Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-008

9 January 2017

[redacted]

Re: CLARIFICATIONS ON THE DATA PRIVACY ACT AND ITS IMPLEMENTING RULES AND REGULATIONS

Dear [redacted]

This pertains to your queries received by the National Privacy Commission (NPC) on 7 November 2016 through email. Specifically, you inquired regarding the following:

a. What is the definition of outsourcing/subcontracting under Rule X? Does outsourcing refer to a function/activity which the Company can perform but decides to allow another person to do it for the Company? Does outsourcing refer to a function/activity which the Company cannot perform or is restricted from performing because it is not in its powers/primary/secondary purpose?
b. What is meant by automated decision-making and profiling under Sec. 34.a.1 vs. automated processing or profiling under Sec. 34.a.2.b? – this is related to automated processing of personal data for profiling or processing for direct marketing and data sharing, under Sec. 19.a.1
c. What is meant by "a report containing aggregated data" under Sec. 41b, Breach report, for security incidents not involving personal data?
d. Why does Data Sharing exclude Outsourcing under Sec. 3f? What does this mean?
e. What is meant by data sharing for "commercial purposes"?
f. What happens if the data is only physically stored to a storage provider who has no access at all to the data? Does this fall within the ambit of the Data Privacy Act?

Outsourcing / Subcontracting

According to Section 9 of the Implementing Rules and Regulations (IRR) of the Data Privacy Act (DPA), a key function of the NPC is to develop rules and regulations for the effective implementation of the law. Pursuant thereto, the Commission issued on 10 October 2016, NPC Circular No. 16-02, which pertains to data sharing agreements involving government

agencies. The issuance applies to personal data under the control or custody of a government agency that is being shared with or transferred to a third party, as well as to personal data under the control or custody of a private entity that is being shared with or transferred to a government agency.[1] Its limited scope notwithstanding, the Circular may be utilized as guidance when taking up data sharing agreements in the private sector, including related concepts such as outsourcing or subcontracting.

On that note, Section 3(d) of the Circular defines outsourcing as the "disclosure or transfer of personal data by a personal information controller to a personal information processor"[2]. Thus, it occurs when a natural or juridical person instructs another to process personal data on its behalf, regardless of the motivation or reason behind such arrangement.

That said, it must be emphasized that the processing of personal data must always be authorized under the DPA.[3] Accordingly, a personal information controller can only perform an operation relative to personal data under its control or custody if it is allowed to do so under the law. Corollarily, only a sanctioned activity or operation may be delegated or subcontracted to another person or organization. Indeed, if a person has no authority to process personal data, it should not be in control or have custody thereof, to begin with.

Automated Decision-making, Automated Processing and Profiling

Section 34.a.1 of the IRR refers to the right of the data subject to be informed of the processing of his or her personal data, including the existence of automated decision-making and profiling. Section 34.a.2.b, on the other hand, pertains to the right of a data subject to be notified of the purpose of the processing (e.g., for profiling, direct marketing, etc.) of his or her personal data, prior to the entry of the latter into the processing system. Finally, Section 19.a.2 involves the general principle in data processing which states that a data subject must be given specific information about the purpose and extent of the processing (including automated processing) of his or her personal data.

Taken together, these provisions emphasize that when a personal information controller is about to process the personal data of an individual, it must make sure that the latter is properly informed of such processing, including the purpose thereof.

For the definitions of the key terms mentioned in the aforesaid provisions, please note the following:

a. *Automated Processing*. The term is not defined in the DPA or its IRR. However, Section 48 of the latter does provide some guidance, *to wit*:

> "Section 48. Notification for Automatic Processing Operations. The personal information controller shall notify the Commission before carrying out any wholly or partly automatic processing operations or set of such operations

[1] NPC Circular No. 2016-02, §2.
[2] NOTE: Under the DPA, a personal information controller refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf, while personal information processor refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
[3] *see*: RA 10173, §12-13.

> intended to serve a single purpose or several related purposes, including passive collection of data." (underscoring supplied)

This may be read together with the 15th preambular clause of the EU Directive 95/46/EC (EU Directive). To recall, the DPA largely based on the language of the Directive. The aforesaid provision states:

> "Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question." (underscoring supplied)

Based on the foregoing provisions, automated processing may be understood as referring to a series or a structured set of processing operations performed on personal data, which is intended to serve a single purpose or several related purposes. The automated or automatic nature of the system indicates that, by design or as intended by the personal information controller or personal information processor, there is limited to no human intervention in the conduct of the processing.

It is important to note that in this system, no decision is made or arrived at relative to the data subjects involved, particularly one that significantly affects his or her rights and interests.

b. *Automated Decision-making*. Although the term is also not specifically defined in the IRR of the DPA, the EU Directive is likewise useful in this regard. Article 15 of the Directive declares:

> "1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc." (underscoring supplied)

As may be gleaned from the provision above, automated decision-making is essentially automated processing that includes or involves a decision or decisions that significantly affect or impact the rights and interests of a data subject.

Thus, where a financial institution conducts automated processing of loan applications (including the personal data of the applicants) that immediately result in the approval or denial of such applications, the company, as personal information controller is considered to be engaged in automated decisionmaking. By contrast, if the applications are merely sorted or classified (e.g., according to type, amount, etc.) by the company upon submission thereof, the latter is viewed as being merely engaged in automated processing.

c. *Profiling*. Profiling refers to any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that person's

performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[4]

While not prohibited by law, profiling is generally frowned upon, especially to the extent that it can negatively impact the rights and interests of data subjects. In many instances, profiling forms part of an automated decision-making system. Thus law mandates that a data subject must be properly informed whenever his or her personal data will be processed for profiling purposes.[5] He or she may also object to the processing of his or her personal data, when it is intended for profiling purposes.[6]

Aggregated Data

Section 41.b of the IRR reads:

> "All security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, the effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall constitute sufficient documentation. These reports shall be made available when requested by the Commission. A general summary of the reports shall be submitted to the Commission annually."

As provided thereunder, "a report containing aggregated data" refers to one which only contains a summary or general description of the security incident. With no personal data involved in this kind of occurrence, it falls outside the scope of the DPA, leaving no need for a detailed account thereof.

Data Sharing vis-à-vis Outsourcing

Data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned.[7] Outsourcing, on the other hand, is the disclosure or transfer of personal data by a personal information controller to a personal information processor,[8] in order for the latter to process the data according to the instructions of the controller.

Based on the foregoing definitions, two (2) key differences exist between data sharing and outsourcing. First, all parties to a data sharing agreement are considered personal information controllers under the law. In a subcontracting or outsourcing agreement, there has to be at least one personal information controller, and one personal information processor. Second, in terms of purpose or objective, each party to a data sharing agreement has its own reason for processing the personal data involved. In a subcontracting or outsourcing agreement, a

[4] IRR of RA 10173, §3(p).
[5] *see*: IRR of RA 10173, §19(a)(2), §34(a)(1), §34(a)(2)(b).
[6] IRR of RA 10173, §34(b).
[7] IRR of RA 10173, §3(f).
[8] Ibid.

personal information processor has no other purpose or objective for processing the personal data other than that imposed by the instructions of the personal information controller.

Data Sharing for "Commercial Purposes"

Data sharing for commercial purpose is data sharing with the purpose of gain or profit. It should be taken in its ordinary meaning.

Physical Storage of Data

Processing is defined as any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data. It may be performed through automated means, or manual processing, if the personal data are contained, or intended to be contained, in a filing system.[9]

Given that storage is within the definition of processing, it is subject to the regulations provided under the DPA.

For your reference.

Sincerely,

JAMAEL A. JACOB
Director, Privacy Policy Office

Approved:

IVY D. PATDU
Deputy Privacy Commissioner,
Policy and Planning

[9] IRR of RA 10173, §3(o).