Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-033

26 November 2018

[redacted]

Re: DATA SHARING, CONSENT, AND COMPLIANCE WITH THE DATA PRIVACY ACT OF 2012

Dear [redacted],

This is in response to your request received by the National Privacy Commission (NPC) concerning various inquiries and clarifications regarding Republic Act No. 10173,[1] known as the Data Privacy Act of 2012 (DPA), particularly, the following:

1. If two PICs agree to share data with a data sharing agreement signed stating that compliance to the Data Privacy Act will be separate responsibilities, will both PICs be held responsible for a violation committed by only one of them if violation involves the shared data (e.g., non-encryption, processing without consent)?

2. Is there any standard as to how a recipient of personal data will ensure that the data to be received is being shared with consent from the data subject? Is a certification/ contract stating that consent from data subjects were obtained sufficient?

3. Is there a benefit in obtaining new consent via SMS or other means of communication (purpose is processing with another PIC/PIP) if the same data subject has previously signed a consent form for the same purpose? Is there any timeline on the validity of a signed consent if nothing is stated in the consent form? As context to the above, a data partner of the company sends SMS opt-in confirmation to potential clients before our company's loan approval. The SMS asks the data subject whether he consents to data partner giving its score to HCPH based on its transaction data with Company A (not the data partner). These data subjects have already signed the HCPH consent form where it states HCPH may collect data from described third-parties.

4. In the context of mobile operators sending SMS messages to its subscribers with direct marketing offers for third party products and services, it is understood that prior consent from the subscribers is required. What practical methods/channels is considered acceptable for obtaining such consent from the existing subscriber base of such mobile operators?

[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 Privacy Commission and for other Purposes [DATA PRIVACY ACT OF 2012], Republic Act No. 10173 (2012).

We provide the following clarifications:

Data sharing and compliance with the DPA

To clarify, all personal information controllers (PICs) and personal information processors (PIPs) are mandated to comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and issuances of the NPC.

PICs that share personal data under a data sharing agreement (DSA) 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.

Data sharing and consent of the data subject

In relation to data sharing arrangement, the DSA or the pertinent contract may stipulate such fact or guarantee that the PIC sharing the personal data has collected or processed such on the basis of any of the criteria for lawful processing of personal and sensitive personal information under Sections 12 and 13 of the DPA, and that the data subject consented to the data sharing, unless consent is not required for the lawful processing of personal data.

Consent

Under Section 3(b) of the DPA, consent is defined as any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.

From the definition provided above, it is clear that consent must be evidenced by written, electronic, or recorded means.[2] Any of the three (3) formats provided may be adopted by a PIC. Nonetheless, it is worth emphasizing that, regardless of the format of the consent given by the data subject, it must be freely given, specific, and informed.[3]

In line with the foregoing discussion, implied, implicit or negative consent is not recognized under the law.

Further, as to whether there is a timeline on the validity of a signed consent if nothing is stated in the consent form, the IRR states that when consent is required, it must be time-bound in relation to the declared, specified and legitimate purpose.[4] The time-bound element does not necessarily mean that a specific date or period of time has to be declared. Thus, for instance, declaring that processing will be carried out for the duration of a contract between the PIC and the data subject may be a valid stipulation.

[2] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §3(c).
[3] *Id.*
[4] *Id.* § 19 (a) (1).

Also, as long as the purpose, scope, method and extent of the processing remains to be the same as that disclosed to the data subject when consent was given, the consent remains to be valid.

Where applicable, such as in cases where the period of processing can be reasonably ascertained at the time of collection, a PIC may specifically provide for the period of validity of a consent obtained from a data subject. The limitation merely emphasizes that consent cannot be overly broad and perpetual for this would undermine the very concept of consent as defined in the law.

We understand that as far as HCPH is concerned, the basis of processing personal data would be the consent of the data subject and/or the contractual relation with the data subject or taking steps at the request of the data subject prior to entering into a contract.

It must be clearly conveyed to the data subject that prior to the loan approval, HCPH would be conducting due diligence and/or further investigation on the applicant-data subject, which will involve collecting further information from third-party sources, and the data subject must consent to the same. Further, these third-party sources must be identified, and the data subject must authorize them to share information with HCPH. Finally, the data subject has to be notified of the transfer of transaction data from Company A to the data partner, the processing done by the data partner and the relationship between the data partner and HCPH, and data subject has to specifically consent and authorize such transfer and processing.

Direct marketing through SMS messages and consent of the data subject

You mentioned that mobile operators would send direct marketing offers for third party products and services via SMS messages to its existing subscriber base. In relation to the same, you inquired on the acceptable practical methods or channels for obtaining consent from the said subscribers.

If consent is the appropriate basis for processing made by the said mobile operators, it is possible for them to obtain consent through an SMS request. For postpaid subscribers, there is an option of sending hardcopy consent forms. Lastly, for those with online accounts with these mobile operators, sending consent forms online through their respective account dashboards or email may also be considered.

The mobile operators should come up with the most efficient and effective way of obtaining consent, taking into consideration the type of processing they will do.

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.) IVY D. PATDU
Officer-in-Charge and
Deputy Privacy Commissioner
for Policies and Planning