Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-30

28 June 2017

[redacted]

Re: CLARIFICATIONS ON THE INTERPRETATION OF THE DATA PRIVACY ACT OF 2012

Dear [redacted]

This is with regard to your queries received by the National Privacy Commission (NPC) on 4 May 2017 with regard to clarifications of certain issues raised during the Data Privacy Act awareness session conducted on 3 May 2017.

Use of a database of personal data

We understand that there may be instances where certain databases of personal data, i.e. list of members of business chambers and their personal contact details, may be acquired or purchased by the bank in good faith from another entity, and thereafter, the bank uses these database for marketing purposes. Later on, the bank discovers that the list came from an unlawful activity, i.e. intentional breach, etc. You would like to clarify the extent of liability of the bank in the said case.

The Data Privacy Act of 2012 (DPA) espouses the general data privacy principles[1] of transparency, legitimate purpose and proportionality. The law likewise provides for the rights of the data subject. All personal information controllers and personal information processors are mandated to adhere to these principles and to uphold the rights of the data subjects in the collection, processing, and retention of personal data.

The law likewise provides for the criteria for lawful processing of personal, sensitive personal and privileged information in Sections 12 and 13 thereof.

[1] RA No. 10173, §11; Implementing Rules and Regulations (IRR), §18

In the scenario given, we believe that the bank should always ensure that the processing it does always adheres to the general data privacy principles and gives due consideration to the rights of data subjects at all times.

Thus, where a bank has reasonable knowledge that a database of personal data it uses for marketing is the fruit of an unlawful activity, we believe that the bank should discontinue from processing such personal data as the same may be construed as unauthorized processing which is punishable under Section 25 the DPA.

Information available in the public domain

You request for guidance on whether consent is required from the data subject to use his or her personal data for marketing purposes when such personal data is available in the public domain, i.e. telephone directory, Facebook, etc.

We believe that the provisions of the DPA are still applicable even for those personal data which are available in the public domain. Note that the law has specified the information which is outside of its scope but only to the minimum extent necessary to achieve the specific purpose, function, or activity in Section 4 thereof.

There is no express mention that personal data which is available publicly is outside of its scope. Thus, "it is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation."[2]

With this, we believe that the PIC which collects and processes personal data from the public domain must still observe the requirements under the law, specifically on the criteria for lawful processing of personal, sensitive personal and privileged information found under Sections 12 and 13 thereof.

Thus, even if the data subject has provided his or her personal data in a publicly accessible platform, this does not mean he or she has given blanket consent for the use of his/her personal data for whatever purposes.[3]

We believe that consent may still be required from the data subject where his or her data will be processed for marketing purposes even if such personal data was procured from the public domain.

We reiterate the definition of consent 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."[4]

[2] Office of the Privacy Commissioner for Personal Data, Hong Kong, *Guidance Note - Guidance on Use of Personal Data Obtained from the Public Domain*, August 2013, available at https://www.pcpd.org.hk/english/publications/files/GN_public_domain_e.pdf
[3] Id.
[4] RA No. 10173, §3(b)

Automated processing/decision-making and the notification requirement

Section 48 of the IRR provides for the notification requirement where a personal information controller is engaged wholly or partly in automated processing, and such processing becomes the sole basis for making decisions which would significantly affect a data subject.

The notification shall include the following information:

1. Purpose of processing;
2. Categories of personal data to undergo processing;
3. Category or categories of data subject;
4. Consent forms or manner of obtaining consent;
5. The recipients or categories of recipients to whom the data are to be disclosed;
6. The length of time the data are to be stored;
7. Methods and logic utilized for automated processing;
8. Decisions relating to the data subject that would be made on the basis of processed data or that would significantly affect the rights and freedoms of data subject; and
9. Names and contact details of the compliance or data protection officer.

The provision above requires all PICs who are engaged in automated processing which leads to automated decision-making that significantly affects a data subject to notify the Commission of the said automated processing operations, i.e. a bank should notify the Commission of its processing systems that are capable of making automated decisions.

The notification may be done once and not every time there is an automated decision made.

Note also that Section 48(b) of the IRR further provides that "no decision with legal effects concerning a data subject shall be made solely on the basis of automated processing without the consent of the data subject."

For your reference.

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman