Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-31

28 June 2017

[redacted]

Re: CONSENT ON THE SHARING OF MOBILE NUMBER OF BANK CLIENTS FOR CREDIT SCORING

Dear [redacted],

This is with regard to your queries received by the National Privacy Commission (NPC) on 9 June 2017. Specifically, you are asking for guidance on a question raised by an entity that provides credit scores on the basis of mobile phone data.

We understand that such entity has growing operations in Vietnam, and is looking at working with a bank and a telecommunications company here in the Philippines. Essentially, the proposed transaction would require the bank to share encrypted information of its client's mobile phone number to the credit scoring entity. The latter will then send this encrypted information to the telecommunications company, whereby the telecommunications company will decrypt these, determine mobile phone behavior, and send the information to the credit scoring entity.

The credit scoring entity will thereafter input these in their algorithm and provide the credit score to the bank. It is claimed that the credit scoring entity will have no access to personal information. You inquire on whether the above proposed transaction is feasible even without the consent of the banks' depositors.

Further, you likewise inquired on anonymization of personal data, and when will such process prevent identifying a particular person owning the data, and does encryption satisfy such process.

Consent and lawful processing of personal information

We consider the bank clients' name and mobile phone numbers as personal information, the processing of which should comply with the provisions of the DPA, its Implementing Rules and Regulations (IRR) and related issuances of the NPC.

Section 3(b) of the Data Privacy Act of 2012 (DPA) provides:

> "(b) Consent of the data subject refers to 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."

In relation to the above, Section 12 of the law provides for the criteria for lawful processing of personal information. As a general rule, the processing of personal information is permitted when at least one of the following conditions exists:

1. The data subject has given his or her consent;
2. The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
3. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
4. The processing is necessary to protect vitally important interests of the data subject, including life and health;
5. The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
6. The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.

We believe that proposed processing and sharing envisioned by the inquiry would fall under the first criteria above, that is processing with the consent of the data subject. Thus, the banks cannot share its clients' mobile phone numbers, even if in encrypted format, to telecommunications company (telco) through the credit scoring entity, and thereafter, the sharing of mobile phone behavior by the telco to the banks, without first securing the clients' consent both by the bank and the telco.

We wish to emphasize that from the definition of consent under the DPA, it is clear that consent given by a data subject must be evidenced by written, electronic, or recorded means. An implied, passive, or negative consent does not meet such a requirement, including one that merely provides an opt-out option (i.e., a data subject is merely notified of the period within which he or she can object to the processing of his or her personal data).

Outsourcing

Aside from the consent requirement, we believe that there is a need to consider the provisions of the IRR on outsourcing or subcontracting as the contractual agreement between the credit scoring entity and the bank may be characterized as such.

Under the IRR, outsourcing or subcontracting is defined as "the disclosure or transfer of personal data by a personal information controller to a personal information processor."[1] PICs are required to "use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes"[2] when outsourcing the processing of personal data.

In this case, the bank should ensure that its contract with the credit scoring entity complies with the IRR's provisions on outsourcing. Refer to Section 44 of the IRR for additional details on outsourcing agreements.

Data Sharing

In addition, we wish to reiterate the provisions of the IRR as well as NPC Circular No. 2016-02 on data sharing and data sharing agreements (where it would involve a government bank).

We believe that data sharing would come into play between the bank and the telco. Note that the bank will essentially be sharing mobile phone numbers to the telco and the latter will then share its subscribers' mobile phone behavior to the bank, where both procedures are to be facilitated by the credit scoring entity.

Note that data sharing in the private sector is allowed provided that there is consent of the data subject, and a data sharing agreement shall cover the data sharing for commercial purposes.[3] Where the data sharing involves a government bank, it must be for the purpose of a public function or provision of a public service and likewise be covered by a data sharing agreement.[4]

Automated Processing

On the processing to be done by the credit scoring entity using its algorithm to provide a credit score to the bank, there may be a need for further information and analysis to determine if the same would constitute automated decision-making.

Under Section 48 of the IRR, the PIC carrying out any automated processing operations or set of such operations shall notify the Commission when the automated

[1] Implementing Rules and Regulations (IRR), RA No. 10173, §3(f)
[2] Id., §43
[3] Id., §20(b)
[4] Id., §20(d)

processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject.

Essentially, where the outsourced processing of personal data to come up with a credit score is deemed to be an automated processing which is the sole basis for a decision significantly affecting a data subject, the bank as the PIC would have to notify the Commission of this data processing system.

Anonymization

Information is anonymous when such information "does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."[5]

Both the Regulation (EU) 2016/679, which repeals the 1995 EU Directive upon which the DPA is based on, recognizes that "the principles of data protection should not apply to anonymous information."[6]

We note also that ISO/IEC 29100 defines anonymization as a process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party.[7]

The goal of anonymization is avoiding identification of individuals by preventing hidden linking of attributes to a data subject.[8]

Encryption, on the other hand, is considered as a security measure or safeguard in the processing of personal data.[9] Encryption "aims to provide the confidentiality of a communication channel between identified parties (human beings, devices, or pieces of software/hardware) to avoid eavesdropping or unintended disclosure."[10]

We understand also that encryption is a pseudonymisation [11] technique, i.e. "encryption with secret key - the holder of the key can trivially re-identify each data subject through decryption of the dataset because the personal data are still contained in the dataset, albeit in an encrypted form. Assuming that a state-of-the-art encryption

[5] Recital 26, Regulation (EU) 2016/679
[6] Regulation (EU) 2016/679 and DIRECTIVE 95/46/EC, Recital 26
[7] ISO/IEC 29100:2011(en), Information technology — Security techniques — Privacy framework, available at https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en
[8] Id.
[9] See Regulation (EU) 2016/679 Recital 83, Article 6(4)(e), 32(1)(a),
[10] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques – ANNEX - A primer on anonymisation techniques, 10 April 2014
[11] Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014. - Pseudonymisation consists of replacing one attribute (typically a unique attribute) in a record by another. The natural person is therefore still likely to be identified indirectly; accordingly, pseudonymisation when used alone will not result in an anonymous dataset.

scheme was applied, decryption can only be possible with the knowledge of the key."[12]

From the foregoing, we believe that encryption is not equivalent to anonymization. Thus, banks sharing encrypted information of its client's mobile phone number is actually sharing personal information notwithstanding its encrypted form.

For your reference.[13]

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[12] Id.
[13] This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.