Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-007

9 January 2017

[redacted]

Re: **CONSENT, COLLECTION OF FEES RELATIVE TO THE RIGHT TO ACCESS AND INCIDENTAL COLLECTION OF PERSONAL DATA**

Dear [redacted],

This pertains to your queries received by the National Privacy Commission (NPC) on 20 and 27 December 2016 by email. Specifically, you raised the following questions:

a. Whether or not the National Privacy Commission considers written consent as best practice in terms of proof the consent given by a data subject?
b. If the processor will use a recording to evidence the presence of consent, will it be easier to convince the Commission that consent is present despite the lack of a signature? What evidence is needed to convince the Commission that the recording embodies the consent of the data subject, especially in cases where the latter alleges that the recording is fraudulent or denies having made any recorded consent at all?
c. Whether or not the NPC will honor or recognize as lawful a policy statement by the personal information processor (PIP) expressly stipulating that inputting any of the requested information serves as consent/waiver of privacy?
d. Whether or not a PIP can charge a reasonable/minimal fee for the data subject's access to his or her personal data?
e. If a service provider (which is not a Business Process Outsourcing [BPO]) collection or processesing personal data or information is merely incidental to the nature of its services, is it still covered by Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA)?

Consent

Under Section 3(b) of the DPA, and Section 3(d) of its Implementing Rules and Regulations (IRR), consent is defined as follows:

> "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." (underscoring supplied)

From the definition provided above, it is clear that consent may be evidenced by written, electronic, or recorded means.[1] Any of the three (3) formats provided may be adopted by a personal information controller (PIC) relative to the collection and processing of personal data. The NPC currently does not maintain any preference among the three. 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.[2]

In line with the foregoing discussion, implied, implicit or negative consent is not recognized under the law. Thus, a company policy that merely stipulates that the inputting of requested personal information amounts to consent or a waiver by a data subject of his or her data privacy rights shall not be considered as valid consent, as required under the DPA.

Regarding consent through recorded means or consent given through a duly recorded oral statement, the PIC is also allowed to present any other types of evidence (i.e., object, documentary, electronic evidence) that may validate the existence and content of the said recording. Note that, pursuant to the Rules of Procedure of the Commission, the Rules of Court shall apply suppletorily whenever practicable and/or convenient, given the circumstances.[3]

As per the Rules of Court, objects, when proffered as evidence, are those addressed to the senses of the court. When an object is relevant to the fact in issue, it may be exhibited to, examined or viewed by a court.[4] Documentary evidence, on the other hand, consists of writing or any material containing letters, words, numbers, figures, symbols or other modes of written expression offered as proof of their contents.[5]

The are also the Rules on Electronic Evidence which apply to electronic documents or electronic data messages offered or used in evidence.[6] An electronic document refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. The term "electronic document" may be used interchangeably with "electronic data message.[7]

Audio, photographic and video evidence of events, acts or transactions are likewise admissible provided that they are shown, presented, or displayed to the court, and identified, explained or authenticated by the person who made the recording or by some

[1] IRR of DPA of 2012, §3(d).
[2] *id.*
[3] NPC Circular 16-04 – Rules of Procedure dated December 15, 2016, §32.
[4] Rules of Court, Rule 130, §1.
[5] *id.*, §2.
[6] A.M. No. 01-7-01-SC - Rules on Electronic Evidence dated July 17, 2001, Rule 1, §1.
[7] *id.*, Rule 2, §1(h).

other person competent to testify on the accuracy thereof.[8] Subject to the same conditions, a recording of a telephone conversation or ephemeral electronic communication may also be admitted in court.[9]

Charging of Fees

The DPA recognizes the data subjects' right to reasonable access, upon demand, to the following:

1. Contents of his or her personal data that were processed;
2. Sources from which personal data were obtained;
3. Names and addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data to recipients, if any;
6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
7. Date when his or her personal data concerning the data subject were last accessed and modified; and
8. The designation, name or identity, and address of the personal information controller.[10]

It is silent on the matter regarding the charging of fees relative to the access by a data subject to his or her personal data.

However, Regulation (EU) 2016/679—which repeals the 1995 EU Directive which the DPA is based on—is instructive in this regard:

> "3. The controller shall provide a copy of the personal data undergoing processing. <u>For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs</u>. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."[11] (underscoring supplied)

Based on the foregoing, we believe that a PIC may charge reasonable fees to defray the costs of reproduction of the personal data being processed by the PIC.

Processing of personal data that is merely incidental to the nature of services offered by a company vis-à-vis scope of the DPA

Section 4 of the DPA provides, as follows:

> "SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information

[8] *id.*, Rule 11, §1.
[9] *id.*, Rule 11, §2.
[10] A.M. No. 01-7-01-SC - Rules on Electronic Evidence dated July 17, 2001, §34(c).
[11] REGULATION (EU) 2016/679, Article 15(3).

> processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph.. xxx"

In addition, Section 4 of the IRR states:

> "Sec. 4. Scope. – The Act and these Rules apply to the processing of personal data by any natural and juridical person in the government or private sector… xxx"

From the above-quoted provisions, it is evident that the law makes no distinction as to the nature of the processing of personal data (i.e., whether or not it is a main or primary activity or merely an incidental one) when delineating the scope of its application. Thus, for as long as a natural or juridical person is engaged in the processing of personal data, it is bound to comply with the provisions of the DPA, unless the data involved falls within the exceptions recognized under the law.

For your reference.

Sincerely,

JAMAEL A. JACOB
Director, Privacy Policy Office

Approved:

IVY D. PATDU
Deputy Privacy Commissioner,
Policy and Planning