Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2020-021[1]

29 May 2020

[redacted]

RE: AUTOMATED RETRIEVAL OF BANK TRANSACTION HISTORY

Dear [redacted]

We write in response to your request for an advisory opinion received by the National Privacy Commission (NPC) which sought to clarify issues on the rights of data subjects and compliance requirements under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC in relation to automated retrieval of data.

We understand that your client, ING Bank N.V. Philippines (ING), a banking entity, operates a mobile banking application (mobile app) that offers digital banking services which shall eventually include consumer loans. In traditional loans, banks require potential borrowers to submit documents to prove good credit standing and their capacity to pay the loan such as pay slips, certificates of employment, income tax returns and bank statements. The loan application process usually takes months, depending on the availability of such documents. Furthermore, banks must also deal with the risk of false or fraudulent documents submitted by potential borrowers.

You further disclosed that ING intends to ease the loan application process by shortening the period of assessment and at the same time, ascertaining the authenticity of the documents submitted. ING, through its mobile app, aims to automate the manual process of requesting for copies of a potential borrower's bank statements from other banks for a faster approval process. The proposed automated retrieval process shall enable potential borrowers to retrieve their transaction history (e.g. date, description of transaction, debit and credit entries and account balance) from other online banking accounts and facilitate immediate submission of the same to ING.

[1] Tags: personal information; lawful criteria for processing; consent; automated retrieval; bank transaction history; loan application; right to access; right to data portability; right to be informed; security measures.

As illustrated in your letter, during the loan application process, potential borrowers can select the specific bank/s from which to retrieve their transaction history by entering the respective online banking account log-in credentials for the said selected bank/s in the ING mobile app.

The ING mobile app shall then access the respective online bank account/s for the sole purpose of extracting the potential borrower's name, account number and transaction history over a twelve-month period or a shorter period, whichever is allowed by the other bank/s. ING shall engage a service provider to provide the technology that will enable the automated retrieval feature of the mobile app. However, the decision on whether a potential borrower's loan application will be granted shall still be done manually by a bank officer, based on the standards set by ING.

You now seek clarification on the following issues:

1) Is authorization under the automated retrieval process an exercise of the rights of the data subjects?; and
2) What are the compliance requirements under the DPA and related issuances of the NPC applicable to the automated retrieval process?

Nature of personal data; processing of personal data; automated retrieval

The DPA defines personal information as any information, whether recorded in a material form or not, from which the identify of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[2]

On the other hand, processing of personal information and sensitive personal information, collectively referred to as personal data, is 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.[3] Given its broad definition, it includes anything that can be done with personal data in any form, including by automated means.

Hence, the name, account number and the bank account transaction history of a potential borrower are considered personal information since it directly identifies a specific individual. The automated retrieval thereof, considered a form of processing, must comply with the standards provided by Section 12 of the DPA.

Exercise of the rights of a data subject; right to access; right to data portability

The rights of a data subject pertaining to access and portability correspond with each other. The right to access allows a data subject reasonable access to, upon demand, the following:

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3 (g) (2012).
[3] *Id.* § 3 (j).

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

On the other hand, the right to data portability is referred to as the right of a data subject to obtain from a personal information controller a copy of his or her personal data that was processed or undergoing processing by the latter, in an electronic or structured format, which is commonly used and allows for further use by the data subject.[5] This right primarily takes into account the right of the data subject to have control over his or her personal data being processed by the personal information controller based on consent or contract, for commercial purpose, through automated means.[6]

Based on the foregoing, data subjects are entitled to have reasonable access to their respective personal data. Upon being given such access, data subjects may request to be given a copy of the data in a portable format where such personal data is being or was processed in an electronic or structured format.

Potential borrowers are considered data subjects not only of ING but also that of other bank/s where they have accounts with. To illustrate, a person applying for a loan with ING who wishes to use his or her bank statements from Bank A to fulfill ING's loan application requirement is a data subject of both ING and Bank A. As a data subject of Bank A, the potential borrower is entitled reasonable access to his or her bank transaction history for a given time period and can also request for copies of his or her transaction history.

In your query, the rights to access and data portability shall be exercised by the data subject through the ING mobile app by entering his or her log-in credentials for the selected bank, Bank A. The mobile app shall then access the said online banking account and retrieve the potential borrower's name, account number and transaction history. ING, through its authorized bank officers, shall then use such information to assess the potential borrower's capacity to pay the loan.

The automated retrieval feature may be considered as an exercise of data subject rights through the ING platform, pursuant to the authority given by the data subjects themselves.

Additionally, ING should take into consideration the requirements under the DPA and related issuances of the NPC which may be applicable to the automated retrieval process. Specifically, the requirements on obtaining consent, the right of data subjects to be informed, adherence to the general data privacy principles, and the safeguards to be implemented to protect personal data against any unauthorized processing.

---

[4] *Id.* § 16 (c).
[5] *Id.* § 18.
[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 36 (2016).

Consent; right to be informed; general data privacy principles; security measures

A data subject is entitled to make an informed decision when it comes to the processing of his or her personal information. Under the DPA, consent should be 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.[7] It may be evidenced by written, electronic or recorded means.[8]

A data subject shall also have the right to be informed whether personal information pertaining to him or her will be, are being, or were processed and pertinent details related thereto.[9]

Hence, a potential borrower must be adequately informed of the processing activity involving his or her personal information and provide consent to ING to access his or her online banking accounts with other banks. As disclosed in your letter, ING shall obtain the consent of potential borrowers in the automated retrieval of their respective personal information.

We note that the act of merely entering the log-in credentials for a particular online banking account does not necessarily equate to the consent required by the DPA. To be considered as valid consent, the potential borrower must be fully informed, among others, of the type of personal information to be processed, how it will be processed, person/s or organization/s in charge of processing and the purpose thereof, prior to entering his or her log-in credentials in the ING mobile app. The data subject shall also have the right to be notified and furnished with the particulars on, among others, the methods utilized for automated access and the extent to which such access is authorized, before the entry of his or her personal information.

In addition, ING's mobile app must have mechanisms to enable the exercise of data subject rights, including the right to object to the processing of their personal data and/or to withdraw consent, where applicable.

We also note that, as mentioned in your letter, all the extracted data will be encrypted, whether the same is at rest or in-transit. Log-in credentials will also be encrypted and shall not be stored. With this, ING should also provide information to the data subjects regarding the storage and retention of the extracted data, details on what will happen to the same should the loan application be denied, and other pertinent information.

Although ING may have legal basis for the lawful processing of the potential borrowers' personal information, it remains subject to the requirements of implementing security measures to protect personal information.

As a personal information controller, ING must still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. As you already mentioned in your letter, ING shall ensure that the general data privacy principles are complied with by informing potential borrowers of the purpose for the processing of their personal information, how such data shall be processed, collecting only what is necessary for the purpose of such processing and that there are no other means to achieve such legitimate

[7] Data Privacy Act of 2012, § 3 (b).
[8] Ibid.
[9] *Id.* § 16 (a-b).

purpose.

ING must implement reasonable and appropriate organizational, technical, and physical security measures to ensure the protection of personal information against any accidental or unlawful destruction, alteration or disclosure and against any other unlawful processing.[10] Considering that ING will be engaging the services of a personal information processor, such arrangement must be covered by an outsourcing agreement or similar agreement to clearly define the legal obligations and liabilities of each party with regard to each other and the data subjects. The service provider must also demonstrate compliance with the DPA.

ING must also take into consideration issues which may be encountered with the proposed automated retrieval system, i.e. access controls, limitations as to accessing the transaction history for the past twelve-month period (or shorter) only, the retention of personal information of potential borrowers who were not approved for the loan application, etc.

Moreover, ING should also conduct a privacy impact assessment to identify and provide an assessment of various privacy risks, and propose measures intended to address and mitigate the effect of these risks on the data subjects.

We emphasize that the DPA, its IRR and other issuances of the NPC do not prohibit banks from implementing innovations to ease banking transactions, provided that the rights of the data subjects are always given paramount consideration.

This opinion is provided based on the 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.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[10] Data Privacy Act of 2012, § 20.