PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2024-004[1]

16 May 2024

[redacted]

Re: ACCESS TO INDIVIDUAL USER ACCOUNTS BY SERVICE PROVIDER

[redacted].:

We respond to your request for an Advisory Opinion on whether the Data Privacy Act of 2012 (DPA)[2] permits an arrangement wherein a service provider such as Smile Technology Pte. Ltd. (Smile) may process personal information and sensitive personal information (collectively, personal data) by accessing individual user accounts from government or financial sites through a separate digital platform.

You state that your client, Smile, is a foreign company that is building a digital platform which provides companies with a unified application programming interface (API) to access the employment and income data of its users. Known as the Smile API, it is a single API for employment and income data in Asia which is accessible through Smile's website or through an integrated widget in the employer or service providers' applications (Third Party Apps). Smile API intends to provide comprehensive and verified employment data to aid banks, financial technology companies (fintechs), recruitment agencies, and other service providers in making informed decisions when evaluating loan applications, credit limits, and job candidates (Applicants).

You further state that Smile shall obtain the consent of the Applicants before processing their personal data, including processing for the purpose of disclosure to third parties. During the account creation process, the Applicants are informed of the nature, purpose and extent of the processing. The Applicants shall then signify their consent by actively checking a tickbox to Smile's Terms and Conditions and Privacy Policy which are readily available through Smile's platforms.

[1] Tags: automated access; personal information processor; consent.
[2] An Act Protecting Individual Personal Information in Information and Communication 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, (2012).

Thereafter, the Applicants shall provide their login credentials and link their accounts to government websites (*e.g.*, Social Security System [SSS] and Philhealth) and other third party platforms via Smile API. Smile shall then use automated means to log in to these sites and extract the Applicants' personal data.

Smile intends to collect and process personal data from various sources such as employment documents, human resource (HR) and payroll systems, gig economy platforms, and social security systems. In addition, Smile will access the Applicants' respective government accounts to retrieve real-time personal data. The personal data that Smile will process are the following:

1. Name
2. Home address
3. Email address
4. Telephone number – work
5. Age
6. Date of birth
7. Marital status
8. Education
9. Photo
10. Offense committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings
11. Information issued by government agencies peculiar to an individual:
    a. Unique identifiers (e.g. Tax Identification Number (TIN), Unified Multipurpose Identification (UMID) number, driver's license number, passport number, Government System Insurance Service (GSIS)/SSS number, voter's registration number, etc.)
    b. Licenses or its denials, expiry, suspension or revocation
    c. Tax returns
    d. Social security contributions
12. Actual and estimated income
13. Profiling and credit scoring data
14. Job performance
15. Social media profiles (e.g. Applicant's account data, user ID, linked accounts, profile information and login credentials)

If the Applicants wish to withdraw their consent, they can easily do so by pressing the "Disconnect Access" button provided in the Smile platforms, including Third Party Apps. Once consent is withdrawn, Smile will delete the personal data from its system within ten (10) minutes.

Thus, you inquire if Smile's access and extraction of personal data to the Applicants' corresponding user accounts, and the subsequent disclosure to its clients and third parties, are compliant with the DPA, its Implementing Rules and Regulations (IRR) and other issuances of the National Privacy Commission (NPC).

Processing based on consent.

Since the dataset that Smile plans to process involves both personal information and sensitive personal information, the processing of the entire data should find lawful basis under Section

13 of the DPA. Specifically, Section 13 (a) allows processing based on consent prior to the processing of personal data.

Consent, as defined under the DPA, is any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal data about and/or relating to him or her.[3] The DPA also requires that consent shall be evidenced by written, electronic or recorded means.[4]

To lawfully process personal data based on consent, Smile needs to guarantee that the consent obtained from the Applicants meets the standards required under the DPA and NPC's issuances.

It is essential that the Applicants are fully informed about how their personal data will be processed. The Applicants should be provided with clear and detailed information regarding the processing of their personal data, as well as any potential consequences that might result from giving their consent. Obtaining consent must be done in an honest and straightforward manner. This means that the information presented to the Applicants while obtaining consent must be communicated in plain and simple language that is easily comprehensible by the intended audience. The Applicants must also be informed of specific processing activities, such as the sharing of personal data with third parties.

It is worth noting that the Applicants, as data subjects, must be given a genuine choice to decline or retract their consent when processing personal data. This implies that the process for refusing or withdrawing consent should be straightforward and free from complicated procedures and requirements at any given time. Further, Smile must ensure that its online portals, through which user consent is obtained, do not employ any design elements or techniques aimed at manipulating or deceiving users into taking any action related to the processing of their personal data.[5] These types of design elements, known as deceptive design patterns, should be avoided.[6]

Smile must also be able to provide another option for those Applicants who do not wish to use the Smile platforms in the processing of their personal data, but still want to pursue their respective transactions/applications with Smile's clients. In such case, these individuals should be informed about other options on how to proceed with their application. Failure to comply with the requirements in obtaining lawful consent may result in possible penalties that may subject Smile to administrative fines or penalties.

Consequently, Smile can process the personal data of the Applicants by accessing their individual user accounts and collecting personal data from external websites, as long as the requirements on obtaining consent are followed. Once lawful consent is obtained, and the Applicants are informed about the nature, extent, and purpose of the disclosure prior to the processing, the subsequent disclosure of the same to clients such as employers and third parties may also be allowed.

Personal information processor; Accountability

---

[3] Data Privacy Act of 2012, Section 3 (b).
[4] Ibid.
[5] National Privacy Commission, Guidelines on Deceptive Design Patterns, NPC Advisory No. 2023-01, Section 2 (A) (7 November 2023).
[6] *Id.* Section 3.tt

A personal information controller (PIC) is an organization that controls the collection, holding, processing or use of personal information.[7] On the other hand, a personal information processor (PIP) is a natural or juridical person to whom a PIC may outsource or instruct the processing of personal data about a data subject.[8]

If a digital platform provider, like Smile, provides employment and income information to assist its clients in making their hiring and loan decisions, then it will be considered as PIP for this specific service.

Be that as it may, Smile must also comply with the requirements provided by the DPA and other relevant rules and regulations similar to a PIC. In addition, a PIP is also bound to adhere to the terms and conditions agreed upon in its contract with the PIC.[9]

As a PIP, one of the basic requirements is for Smile to designate a data protection officer (DPO) in the Philippines and register its processing systems with the NPC. Even though Smile is a foreign corporation and its processing activities happen outside of the Philippines, it is still obligated to comply with the DPA since it processes the personal information of Philippine citizens and residents.[10] Moreover, Smile must also comply with NPC Circular No. 2022-04 on the registration of personal data processing systems, a copy of which is available at https://privacy.gov.ph/wp-content/uploads/2023/05/Circular-2022-04-2.pdf.

Smile should also perform regular privacy impact assessments (PIA) to identify and evaluate potential privacy risks. These assessments should suggest measures to address and reduce the impact of these risks on the individuals whose data is being processed.

We highly recommend that a written agreement be executed between Smile and its PICs to ensure accountability in its processing. This agreement should clearly outline the obligations and liabilities of all parties involved, including their responsibilities to the data subjects.

We emphasize that if Smile processes personal data for any purpose other than providing useful information to its PICs, then it becomes a PIC for that specific processing activity. Consequently, Smile shall assume the concomitant obligations of a PIC under the DPA.

Rights of the data subject; data portability;
retention policy; right to object

The Applicants using the Smile API must be informed of their rights as data subjects and given the opportunity to exercise them. Considering that the processing of personal data is based on consent, we emphasize its significance on the rights to access, object and data portability.

The right to access and portability are interrelated. The right to access allows a data subject reasonable access to, upon demand, the following:

1. Contents of his or her personal information that were processed;

[7] *Id.* Section 3 (h).
[8] *Id.* Section 3 (i).
[9] Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012" [Implementing Rules and Regulations of Data Privacy Act of 2012], Section 45 (2016).
[10] Data Privacy Act of 2012, Section 6 (b).

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, name or identity and address of the personal information controller.[11]

The right to data portability gives individuals the ability to obtain a copy of their personal data that has been processed or is being processed by a PIC in a commonly used electronic format that can be further used by the individual.[12] This right is based on the principle that individuals have the right to maintain control over their personal data that is being processed by a PIC, either through consent or contract, for commercial purposes, or through automated means.[13]

Individuals also have the right to object to the processing of their personal data. In case there is a significant change in the information that was provided to the data subject in a consent form, privacy notice or any similar communication, the data subject should be notified and allowed to object or withdraw their consent for the processing of their personal data.[14] Once a person withdraws their consent, any processing of their data must stop immediately, unless there are other lawful bases to continue. If personal information has already been shared with third parties with the consent of the person, they must immediately be informed of the objection.

It is important to note that the Applicants for employment or loans are considered as data subjects not only of Smile but also of the entities who engaged Smile for this specific purpose, and the corresponding organizations from which their personal data will be obtained (e.g., SSS, GSIS, Philhealth, etc.). For instance, when an individual uses Smile's platforms to apply for a job at Company A, they become a data subject of Smile and Company A. They also remain as data subjects of the organizations that Smile can access through the Applicant's accounts. However, it is important to note that, as the Applicants are utilizing the Smile API, Smile must allow them to exercise their data subject rights, and that they must have a mechanism in which these rights may be exercised.

General data privacy principles; Security measures

Personal data should only be collected for specified and legitimate purposes, which must be declared beforehand, and processed in a way that is compatible with the declared and specific purpose.[15] It is also crucial to maintain accurate and relevant personal data at all times.[16] Personal data processed should be proportionate, adequate and not excessive, limited to what is necessary for the intended purpose.[17] Moreover, personal data collected must be retained

[11] *Id*. Section 16 (c).
[12] *Id*. Section 18.
[13] Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 36.
[14] *Id*. Section 34 (d).
[15] Data Privacy Act of 2012, Section 11 (a).
[16] *Id*. Section 11 (c).
[17] *Id*. Section 11 (d).

only for as long as necessary for the fulfillment of the purposes for which the data was obtained.[18]

Thus, Smile must ensure that the processing of personal data is limited to the purpose of assessing an individual's eligibility for employment or loan. It is also important for Smile to have a retention policy on the personal data within its custody. This includes the retention of personal data of persons whose applications were not successful or did not proceed.

PIPs, like Smile, must also implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the personal data under its custody. Furthermore, Smile is also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[19] Smile may consider industry best practices in the implementation of security measures.

In terms of compliance with the DPA, it is important to note that this is an ongoing process that requires regular evaluation of the effectiveness of security measures against current and potential risks. Furthermore, it is important to emphasize that a PIP's main objective should not be solely focused on compliance. Compliance is achieved when personal data is protected, and the rights of data subjects are upheld through appropriate and reasonable security measures.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

For your reference.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office

---

[18] *Id.* Section 11 (e).
[19] Data Privacy Act of 2012, Section 20 (c) (4).