PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2023-025[1]

29 December 2023

[redacted]

Re: MULTI FACE ID INITIATIVE FOR FRAUD PREVENTION

Dear [redacted]:

We respond to your request for an Advisory Opinion regarding the Multi Face ID initiative by CIBI Information Inc. (CIBI).

We gather from your request that CIBI aims to be the trusted partner of businesses and consumers for their hiring and lending needs by offering technology solutions to solve customer problems across hiring, lending, and partnering. The goal of CIBI is to assist individuals and organizations (hereafter referred to as "CIBI members") in optimizing their risk-based credit and hiring decisions through its "proprietary datasets" to be collected from the CIBI members' customers, borrowers or applicants.

You state that CIBI intends to pursue a project to assist and improve the Philippine financial technology (FinTech) industry in identity mapping and fraud prevention at the onboarding level (the "Project"). The aim is to enable its members by delivering a tool which will provide face recognition on a consortium level supported by a third-party who can provide real-time identity checks. Further, the proposed arrangement is for the FinTech members to contribute the datapoints to CIBI with the latter acting as custodian of the information. CIBI shall then deliver the results to the members who wish to check the accuracy of the application and the consistency of the submitted information.

You further state that as the custodian of information, CIBI undertakes to limit access to only select individuals within the organization. In turn, such individuals shall only release the information to a requesting member following best practices that will protect the data. In addition, only members who contribute data shall be allowed access.

[1] Tags: facial recognition, personal information, sensitive personal information.

Your letter also provides that CIBI will establish the following safeguards and features in the implementation of the Project to comply with the Data Privacy Act of 2012 (DPA):[2]

a) Every data point submitted by the members will be owned by them, not by CIBI;
b) CIBI will only store information in the cloud with all the required security measures following the SOC 2 standards which covers implementation of encryption and data security;
c) CIBI will not disclose the full database to any of the members, only on a per pull basis;
d) Members will obtain the required data consent from their customers and comply with the DPA;
e) Members will be responsible for adhering to strict security and privacy standards when using the product;
f) Members will only use the product for its own legitimate business and operation purposes (account opening, credit/loan applications, financing applications, etc.);
g) CIBI will implement Role-Based Access Control (RBAC) to limit access to data based on job responsibilities (i.e, certain user types cannot access certain product features and data);
h) CIBI will regularly conduct information security training and will remain compliant with the DPA; and
i) CIBI and each of the members will enter into a data sharing agreement (DSA) and a specific contract which will include the safeguards and features in place.

In line with the above, you specifically ask the following:

i) Can the participating Fintechs or banks share the following data points to CIBI for the purpose of establishing a database for fraud prevention in the initial stages of application: a) an individual's full name; b) date of birth; c) photo of individual's face; and
ii) Are the proposed safeguards and features compliant with the DPA?

Personal information; sensitive personal information; biometrics; lawful basis.

The DPA applies to the processing of all types of personal information and sensitive personal information (collectively, personal data). Personal information is defined as any information whether recorded in a material form or not, from which the identity of the 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.[3]

The full name of an individual is considered personal information. A photo of an individual's face, a form of biometric data, is also considered personal information since it directly and certainly identifies a particular individual. In Advisory Opinion No. 2017-063[4] we discussed the nature of biometrics as personal information, *viz.*:

[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, (2012).
[3] *Id. § 3(g).*
[4] NPC Advisory Opinion No. 2017-063, (09 February 2017).

As can be gleaned from Republic Act (RA) No. 10367,[3] biometrics refer to "the quantitative analysis that provides a positive identification of an individual such as voice, photograph, fingerprint, signature, iris and/or such other identifiable features."[4]

While under Article 29 Opinion 4/2007 (EU)[5], a biometric data may be considered both as content of the information about a particular individual as well as an element to establish a link between one piece of information and the individual. As such, it can work as "identifier" for it produces a unique link to a specific individual.

On that note, it must be emphasized that DPA defines personal information as "any information whether recorded in a material form or not, from which the identity 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."[6] Corollarily, hand-written signatures, as may be used to identify an individual, is considered as personal information.

In the same manner, unique information relating[7] to an individual or when linked with other information will allow an individual to be distinguished from others, may be treated as personal information.

Thus, the processing of an individual's full name and photo must find lawful basis under Section 12 of the DPA.

On the other hand, date of birth is considered sensitive personal information as provided under Section 3(l)(1) of the DPA. Considering that the data set intended to be shared includes sensitive personal information, the processing of the entire data may find lawful basis under Section 13 of the DPA. It appears that Sections 13 (a) and 13 (f) of the DPA are the most appropriate lawful bases for the intended processing, *viz.:*

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given his or her consent prior to processing;

xxx

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.[5]

Naturally, the easiest way to facilitate the lawful sharing of personal data among the participating members and CIBI is to obtain the consent of the individual clients. Consent is defined under the DPA 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.[6] Thus, prior to the sharing of personal data, the participating CIBI member must inform its individual clients in clear and concise language of the intent to share their personal data to CIBI, its purpose of creating a database with facial recognition features and relevant details involved in the processing. The individual clients' consent must be evidenced by written, electronic or recorded means pursuant to the requirement of the DPA.

[5] Data Privacy Act of 2012, § 13(f).
[6] *Id.* § 3 (b).

But if the individual clients refuse to give their consent, CIBI may then rely on Section 13 (f) which considers processing pursuant to the establishment of legal claims as lawful basis for processing.

In *BGM v. IPP*[7], we had the occasion to clarify the nature of processing pursuant to Section 13(f), mainly:

> x x x. Its requirement of compelling Complainant to produce a court order prior to the release of the requested information creates a high barrier that effectively impedes the rights vested by the DPA to the latter as a data subject.
>
> Further, Respondent's assertion that the information within its custody can only be disclosed upon data subject's consent or on the basis of a lawful order is misplaced. x x x
>
> In the case of NPC 17-018 dated 15 July 2019, this Commission held that "processing as necessary for the establishment of legal claims" does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of "establishment ... of legal claims" presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established."
>
> This Commission in the same case went on further and held that: The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is "necessary" or may or may not be collected by lawyers for purposes of building a case, applying the qualifier "necessary" to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of "establishment of legal claims" consistent with the general principles of legitimate purpose and proportionality. As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.
>
> Based on the foregoing, the disclosure to be made by the Respondent of the information of the recipient of Complainant's personal information, for purposes of identification of the person liable for the alleged fraud, sans the latter's consent, is necessary for the protection of the lawful rights and interests of the Complainant as contemplated by Section 13 (f) of the DPA. (underscoring supplied)

Based on the above, fraud prevention may be considered a legal claim being established by the CIBI member. Consequently, the processing of sensitive personal information pursuant thereto may be allowed.

General data privacy principles; security measures

While the disclosure of personal data is supported by a lawful basis, CIBI members, as PICs of its clients' personal data, still have the obligation to comply with the other requirements of the DPA. Personal data must be processed lawfully and fairly with strict adherence to the general data privacy principles.

[7] National Privacy Commission, BGM v. IPP [NPC 19-653] (Dec. 17, 2020).

Personal data must be collected for specified and legitimate purposes which must be determined and declared beforehand and processed only in a way that is compatible with such declared and specific purpose.[8] Further, PICs must ensure that personal data is accurate and relevant at all times.[9] Personal data processed should be proportionate, adequate and not excessive in relation to the purposes for which they were collected.[10] To reiterate, data subjects must be aware of the nature, purpose and extent of the processing of his or her personal data, including the risks and safeguards involved and their rights as data subjects, among others.[11]

Thus, CIBI members must comply with the above requirements in the sharing of its clients' personal data to CIBI. CIBI should inform its clients that the sharing is limited only for purposes of establishing a database to prevent fraud, and that disclosed data shall only be limited to the datapoints necessary for the creation of the database (*i.e.*, full name, date of birth and photo of the client's face).

Please note that once CIBI has received the personal data from its members, CIBI shall also be considered as a PIC. Hence, CIBI must also comply with the above requirements. In addition, CIBI must retain only such personal data for as long as necessary or once the fulfillment of the declared purpose has been achieved, unless such retention is required by other laws. This means that there must be a retention policy regarding the personal data stored in the database.

In addition, the data sharing agreement between CIBI and the participating IT-BPO companies should clearly provide for the party's obligations and liabilities not only to each other as contracting parties but to the data subjects as well. This will enable the principle of accountability on the part of CIBI and its members to its data subjects. The same also applies to outsourcing service agreements or similar agreements with service providers that will be engaged in the creation of the database.

PICs are also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the processed personal data. Furthermore, personal information controllers are also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[12]

Regarding your second query on whether CIBI's proposed safeguards and features comply with the DPA, we note that the proposed safeguards and features of the Project can be considered physical, organizational, and technical security measures. To determine if the proposed measures are appropriate with the processing of personal data, factors such as the nature of the personal data to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security information must be considered.[13] These factors will determine if the personal data subject of processing will be kept safe and well protected.

[8] Data Privacy Act of 2012, § 11 (a).
[9] *Id.*
[10] *Id.*
[11] 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] (2016).
[12] Data Privacy Act of 2012, § 20 (c) (4).
[13] *Id.* § 20 (c).

On whether the proposed safeguards are compliant with the DPA, we wish to clarify that compliance does not end once security measures have been put in place. Compliance is a continuing process, involving regular evaluation on the safeguards' effectivity against encountered and projected risks and threats. We would like to note that a PIC's primary objective should not just be mere compliance with the DPA; instead, a PIC should always make sure that personal data are protected through appropriate and reasonable security measures.

We also recommend conducting a privacy impact assessment (PIA) prior to the launch of the Project to identify potential privacy risks to the data subjects. A PIA is a process used to assess and manage the impacts on privacy of a particular program, project, measure, system or technology product of a personal information controller or a personal information processor.

Lastly, the personal information controller must also establish a mechanism for data subjects to exercise their rights. This mechanism should inform data subjects about their rights under the DPA and the degree of control they have over their data, among others. This mechanism may be lodged with CIBI's Data Protection Officer or with the process owner in charge of implementing the proposed processing system.

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