PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2023-026[1]

29 December 2023

[redacted]

Re: CREATION OF A SHARED EMPLOYEE FRAUD DATABASE

Dear [redacted]:

We respond to your request for an Advisory Opinion on CIBI Information, Inc.'s (CIBI) initiative to establish an Employee Fraud Database to prevent and detect fraud that may be perpetuated against employers.

In your letter, you mentioned that a common concern amongst various Information Technology Business Process Outsourcing (IT-BPO) Companies involve employees losing or not returning office-issued equipment. In certain instances, some employees simply disappear and omit the offboarding process. This prompted CIBI to propose the idea of an Employee Fraud Database (the "Project") to its client-members belonging to the IT-BPO sector.

Under the Project, the IT-BPO Companies will provide data points on concerned employees to CIBI. CIBI will then act as the custodian of the submitted information and deliver the results to its members who want to verify if a prospective applicant has committed fraud or any other detrimental act to any employer in the past.

As the custodian of information, CIBI undertakes to limit the access to the database to only a select group of individuals within the organization. These individuals will only release information to requesting members while following the best practices to protect data. Additionally, only CIBI members who contribute data will be granted access to the information.

Your also mentioned that CIBI will establish the following safeguards and features in the implementation of the Employee Fraud Database to comply with the Data Privacy Act of 2012 (DPA):

[1] Tags: sensitive personal information; fraud prevention; legal claims.

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 (preventing fraud and instances of qualified theft);
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 now ask the following:

i) Can the participating IT-BPO Companies share the following datapoints to CIBI for the purpose of establishing a database for fraud prevention and detection which may be perpetuated against employers: a) an individual's full name; b) date of birth; c) whether or not the individual has committed fraud or is under investigation for the possible commission thereof; and
ii) Are the proposed safeguards and features compliant with the DPA?

Personal information; sensitive personal information; lawful basis; shared database of employees.

The DPA considers the name of an individual as personal information. Thus, the processing thereof must comply with the requirements of Section 12 of the DPA.

On the other hand, an individual's date of birth is considered sensitive personal information. The same applies to data relating to an individual's commission of fraud or the fact that an individual is involved in an investigation for the possible commission of fraud.[2]

It must be noted that the data set intended to be shared includes sensitive personal information. As such, the entire data set may be treated as sensitive personal information and, thus, draw the basis for its processing under Section 13 of the DPA. In particular, Section 13 (f) on processing for the establishment of legal claims appears to be applicable, *viz.*:

> SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

[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 (l) (2) (2012).

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.[3] (Underscoring supplied)

In *BGM v. IPP*, the National Privacy Commission (NPC) explained the nature of processing pursuant to Section 13(f):

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.[4]

Relevant also to the Project is the concept of blacklisting as discussed in Advisory Opinion No. 2017-063, *viz*.:[5]

As a generic approach, blacklists are databases that consist of collected specific information relating to a specific group of persons, which may generally imply adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.

That said, blacklisting constitutes processing of personal data and is therefore subject to the general data privacy principles set out in the Data Privacy Act of 2012 (DPA). Thus, the law mandates that a data subject must be properly informed of the nature, purpose and extent of the processing of his or her personal data.
Further, it is mandatory for an organization to clearly establish procedures that allow data subjects to exercise their right to access, rectification, erasure or blocking.

[3] Data Privacy Act of 2012, § 13(f).
[4] National Privacy Commission, BGM v. IPP [NPC 19-653] (Dec. 17, 2020).
[5] National Privacy Commission, Advisory Opinion No. 2017-063 (Oct. 9, 2017) citing Article 29 of Directive 95/46/EC "Working document on Blacklists", Adopted on 3 October 2002 available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp65_en.pdf

Applying the foregoing to CIBI's Project, the proposed sharing of data by an IT-BPO Company with CIBI can be considered processing for the purpose of establishing, exercising or defending a legal claim involving a fraudulent act. Consequently, the processing of such sensitive personal information pursuant to such purpose is allowed under the DPA. Nevertheless, while it cannot be gainsaid that a shared database for fraud prevention could potentially improve the operations and integrity of IT-BPO companies, it is also crucial to balance its potential legal implications to the rights and freedoms of the individuals included in the database.

General data privacy principles; lawful processing; appropriate and reasonable security measures; privacy impact assessment

Although the disclosure of personal data may be supported by a lawful basis, the IT-BPO Companies, who act as personal information controllers of their employees' personal data, are still required to comply with other requirements of the DPA. The personal data should be processed lawfully and fairly with strict adherence to the general data privacy principles.

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.[6] In this particular context, we emphasize that personal information controllers must ensure that personal data is accurate, relevant and up to date at all times.[7] Inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.[8]

We emphasize that the processing of personal data must be proportionate, adequate and not excessive in relation to the intended purposes for which it was processed.[9] This means that the personal data that can be shared by the IT-BPO companies should be limited only to the data points mentioned or only such personal data that are necessary to create the proposed Employee Fraud Database.

Further, 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, their rights as data subjects, among others.[10] Mechanisms for rectifying or deleting inaccurate or irrelevant personal data must also be provided to data subjects.

In sum, the IT-BPO Companies must comply with the above requirements when sharing its employees' personal data to CIBI. The participating IT-BPO Companies should inform its employees that the sharing is limited only for purposes of establishing a database to prevent fraud and that the data that will be disclosed shall only be limited to the data points necessary for the creation of the database.

[6] Data Privacy Act of 2012, § 11 (a).
[7] *Id.* § 11 (c).
[8] Ibid.
[9] *Id.*
[10] 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).

Please note that once CIBI has received the personal data from the participating IT-BPO Companies, it shall also be considered as a personal information controller. 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.

CIBI is also required to implement reasonable and appropriate physical, organizational and technical security measures to ensure the protection of the personal data that was shared by the IT-BPO companies. Furthermore, personal information controllers are also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents that may lead to security breaches.[11]

As to your second query on whether CIBI's proposed safeguards and features for the Employee Fraud Database comply with the DPA, please note that these safeguards and features can be classified as 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.[12] These factors will determine if the personal data subject of processing shall be kept safe and well protected.

We also emphasize that compliance does not end once security measures have been put in place. Compliance is a continuing process, involving regular evaluation on the safeguards' effectiveness against encountered and projected risks and threats. Please also 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.

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.

We also recommend conducting a privacy impact assessment (PIA) prior to the launch of the Employee Fraud database 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. It takes into consideration the nature of the personal data to be protected, the personal data flow, the risks to privacy and security caused by the processing, current data privacy best practices, the cost of security implementation and, where applicable, the size of the organization, its resources and the complexity of its operations.[13] The frequency of the conduct of a PIA shall depend on, among others, how often the proposed database is being updated (*i.e.,* the introduction of new features).

[11] Data Privacy Act of 2012, § 20 (c) (4).
[12] *Id.* § 20 (c).
[13] NPC Advisory No. 2017-03, Guidelines on Privacy Impact Assessment, 31 July 2017.

IT-BPO Companies and CIBI must also establish a mechanism for the exercise of data subject rights. This mechanism should inform data subjects about their rights under the DPA and the level of control they have over their data.

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