Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-32

07 July 2017

[redacted]

Re: CRITICAL INCIDENT REPORT PROJECT

Dear [redacted],

This has reference to your inquiry received by the National Privacy Commission (NPC) on 9 June 2017, wherein you raised your concern on the Critical Incident Report Project (Project) being implemented by a BPO company. We understand that the project is essentially a centralized database containing information of current and former employees, including information on any fraud-related internal disciplinary proceedings against said employees and any civil and/or criminal cases arising therefrom.

The BPO company requires its employees to sign a waiver that will allow the company to collect, update, access, use, retain and process various personal and sensitive personal information, even after termination of employment, for purposes of employee identification, verification, background checking and other legitimate business purpose.

You asked if the said project if legal given that it would seem that the company would be collecting too much information, and if you as an employee may be fired for declining to sign the waiver. You likewise mentioned that the company has not provided you with access to its privacy notice.

Lawful processing of personal data

Processing of personal and sensitive personal information should adhere to the principles of transparency, legitimate purpose and proportionality[1].

The principle of proportionality is particularly critical in this case. Section 18 of the Implementing Rules and Regulations (IRR) of the Data Privacy Act of 2012 (DPA) describes this principle: "the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be

[1] See RA No. 10173, §11 and Implementing Rules and Regulations (IRR) of RA No. 10173, §18

processed only if the purpose of the processing could not reasonably be fulfilled by other means."

Given the scope of the Project, it would seem that there may be other available means through which its purpose of protecting the BPO industry from fraud may be achieved (e.g., implementing stricter employment requirements, requiring applicants to submit a notarized undertaking and attest to the validity of the documents furnished, securing the recommendations or comments of former employers, etc.).

Consent

We wish to emphasize the definition of consent under the DPA – "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."[2]

In the case of the requirement to sign the waiver, the BPO company has the management prerogative to require the same as a pre-employment requirement or a condition for continuation of employment, subject to labor laws and fair employment practices.

We understand that the waiver will allow the company to "collect, update, access, use, retain and process various personal and sensitive personal information, even after termination of employment, for purposes of employee identification, verification, background checking and other legitimate business purpose."

However, we believe that the statement "other legitimate business purpose" must be further defined and made more specific as the contents of the waiver should be unambiguous and must strictly adhere to the general principles in collection, processing and retention stated in Section 19 of the IRR:

1. Collection must be for a declared, specified, and legitimate purpose;
2. Personal data shall be processed fairly and lawfully;
3. Processing should ensure data quality;
4. Personal data shall not be retained longer than necessary; and
5. Any authorized further processing shall have adequate safeguards.

If otherwise, there may be basis to argue that there was no freely given, specific, and informed consent.

Rights of the data subject

Concomitant to the above, the BPO company, as a personal information controller, is required to uphold the rights of data subjects, and adhere to general data privacy principles and the requirements of lawful processing.[3]

With this, we believe that it is well within your right as the data subject-employee to have access to your personal data submitted to the centralized database, to dispute any inaccuracy or error in said personal data, request the BPO company to correct it, and inform recipients or

[2] RA No. 10173, §3(b)

[3] IRR, §6(a)

third parties who have previously received such data of its inaccuracy and its subsequent rectification, to request for erasure of personal data under certain circumstances, *i.e.* personal data is incomplete, outdated, false, unlawfully obtained, used for unauthorized purpose, among others.[4]

You also have the right to be notified and furnished with information on the recipients or classes of recipients to whom your personal data are disclosed as well as reasonable access to the names and addresses of recipients of your personal data and the reasons for the disclosure of your personal data to said recipients.[5]

We also would wish to emphasize that "any doubt in the interpretation of any provision of this Act shall be liberally interpreted in a manner mindful of the rights and interests of the individual about whom personal information is processed."[6]

This advisory opinion is based on the limited information provided in the questions, and may vary based on additional information or when the facts are changed or elaborated.

For your reference.

Very truly yours,

RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[4] See IRR, §34
[5] Id.
[6] RA No. 10173, §38