Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: INFOSYS BPM-PHILIPPINES **NPC BN 18-217**

x----------x

RESOLUTION

AGUIRRE, D.P.C.:

This Resolution refers to the Breach Notification Report[1] dated 24 October 2018 submitted by Infosys BPM-Philippines (Infosys) to this Commission.

The Facts

On 24 October 2018, a Human Resource (HR) personnel from Compensation and Benefits unintentionally disclosed the Marital Status of a fellow employee to unauthorized individuals via e-mail.[2]

On 26 October 2018, or two (2) days after the incident, the affected employee filed a complaint with the HR and Legal Department about the incident. The Corporate Counsel then forwarded the complaint to the Data Protection Officer (DPO) for further investigation.[3] On the same day, the DPO called each of the nine (9) unauthorized recipients of the e-mail, and notified them to sensitize, not to forward, and ensure the deletion of the e-mail.[4] Furthermore, an incident report was also logged in the incident management tool of the company to formalize the complaint and started the investigation.[5]

On 30 October 2018, as part of the investigation, the DPO had a meeting with the affected employee and assured her that her concern is being handled accordingly.[6]

---

[1] Annual Security Incident Report (Data Breach Information) dated 24 October 2018 submitted by Infosys BPM- Philippines.
[2] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*
[6] *Ibid.*

Infosys also reported that the effects or consequences of the incident are: (1) privacy breach of confidential information, and (2) employee dissatisfaction.[7]

Lastly, Infosys enumerated the remedial steps it has undertaken to address the incident:

(1) The DPO called all the unauthorized recipients of the e-mail to notify them not to forward and ensure the deletion of said mail;
(2) A Notice to Explain was issued to the erring employee who was given five (5) days from receipt to comply with the same;
(3) An administrative hearing was conducted for the alleged offense of Serious Violation of the company Code of Conduct;
(4) The unauthorized recipients of the e-mail were asked to sign a non-disclosure agreement;
(5) A disciplinary sanction was given to the erring employee; and
(6) Further awareness on Data Privacy is being conducted across the organization.

Issues

1. Whether there was a personal data breach; and
2. Whether the remedial measures implemented by Infosys BPM Philippines were sufficient to address and prevent the recurrence of the incident.

Discussion

There was a personal data breach.

This Commission finds Infosys to have committed a personal data breach.

Section 3(F) of NPC Circular 16-03 provides that:

> "Personal data breach" refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, **unauthorized disclosure of, or access to, personal data** transmitted, stored, or otherwise processed. A personal data breach may be in the nature of:

[7] *Ibid.*

> 1. An availability breach resulting from loss, accidental or unlawful destruction of personal data;
> 2. Integrity breach resulting from alteration of personal data; and/or
> **3. A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.**[8]

In this case, there was unauthorized disclosure of an employee's sensitive personal information, which is the latter's marital status.

Hence, a personal data breach has been committed.

This Commission notes that Infosys failed to submit its Full Breach Report on the subject incident, as required by Section 17(C) of NPC Circular 16-03. It provides that:

> There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the Commission shall be notified within the 72-hour period based on available information. **The full report of the personal data breach must be submitted within five (5) days**, unless the personal information controller is granted additional time by the Commission to comply.[9]

Section 17(D) of the same Circular provides the necessary information for a Full Breach Report, thus:

> A. The notification shall include, but not be limited to:
>
> **1. Nature of the Breach**
> a. description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;
> b. a chronology of the events leading up to the loss of control over the personal data;
> c. approximate number of data subjects or records involved;
> d. description or nature of the personal data breach;
> e. description of the likely consequences of the personal data breach; and

[8] Emphasis supplied.
[9] Emphasis supplied.

f. name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

a. description of sensitive personal information involved; and
b. description of other information involved that may be used to enable identity fraud.

3. Measures Taken to Address the Breach

a. description of the measures taken or proposed to be taken to address the breach;
b. actions being taken to secure or recover the personal data that were compromised;
c. actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident;
d. action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification;
e. the measures being taken to prevent a recurrence of the incident.

The Commission reserves the right to require additional information, if necessary.[10]

The remedial measures implemented by Infosys BPM-Philippines were sufficient to address and prevent the recurrence of the incident.

Nevertheless, the Commission notes that the Initial Report contained the necessary information of a Full Breach Report and acknowledges the remedial measures taken by Infosys to address the breach incident and protect the personal information of the affected data subject. Aside from this, it is noteworthy that the DPO communicated with the unauthorized recipients of the disclosed personal data and they were asked to sign a non-disclosure agreement.

Furthermore, the administrative hearing that was conducted, the disciplinary sanction that was imposed upon the erring employee, and the conduct of Data Privacy awareness activity across the

[10] Emphasis supplied.

organization were important steps to prevent the recurrence of the incident.

Considering the actions taken by Infosys, the Commission will no longer require it to submit a full breach report.

Nevertheless, the Commission expects Infosys to take the necessary steps to ensure not only that this situation will not be repeated, but, more importantly, that it will be in a better position to safeguard the personal information of its data subjects. Infosys is sternly warned that a similar case in the future will be dealt with more severely.

WHEREFORE, premises considered, this Commission hereby resolves that the instant case NPC BN 18-217 "In re: Infosys BPM-Philippines" is considered **CLOSED** and **TERMINATED**.

Infosys BPM-Philippines is given a **STERN WARNING** that a repetition of similar instances violative of the right of data subjects or a similar conduct or infraction shall be dealt with more severely.

SO ORDERED.

Pasay City, Philippines;
17 December 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

AO
Data Protection Officer

COMPLIANCE AND MONITORING DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission