Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: ACESITE (PHILS.) HOTEL CORPORATION **NPC BN 18-037**

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

RESOLUTION

NAGA, D.P.C.:

This Resolution refers to the data breach notification report dated 21 March 2018 that the Commission received from Acesite (Phils.) Hotel Corporation (Acesite) in relation to the loss of personal data caused by fire.

The Facts

On 18 March 2018, a significant portion of the Hotel was razed by fire.

According to the report of the Bureau of the Fire Protection, the fire was caused by high-temperature electric discharge of a wiring inside the ceiling near the slot machine area, which resulted in short circuit accompanied by a massive electrical ignition. Further, the detected electric default was caused by prolonged usage and normal wear and tear of conductive material of the electrical wiring.[1]

The significant portion of the Hotel was affected by the fire and caused damages to the properties of the Hotel including several records containing data relating to the Hotel's operations, guests, and employees, among others. According to Acesite, the

[1]Galupo, R. (2018). *Hotel fire accidental – BFP*. Retrieved from https://www.philstar.com/nation/2018/09/06/1849003/manila-pavilion-hotel-fire-accidental-bfp#:~:text=MANILA%2C%20Philippines%20%E2%80%94%20The%20Bureau%20of,wiring%E2%80%9D%20and%20deemed%20the%20investigation

personal data possibly involved in the breach cause by the incident includes:

1. Name of guest and employees;
2. Contact Numbers;
3. Email Addresses;
4. Copies of IDs and Passports;
5. Credit Card Details: Name of Cardholder Masked Card Numbers Signature of the Guest; and
6. Employee Payroll Details:
   - Employee ID Numbers
   - SSS Contributions
   - HDMF Contributions
   - Philhealth Contributions
   - SSS ID Numbers
   - Tax Identification Numbers Pag-ibig (HDMF) Numbers.[2]

On 21 March 2018, Acesite sent a notification on the incident, which informed the Commission that the Hotel shall be temporarily inaccessible and non-operational.

On 29 August 2019, Acesite submitted its Full Breach Report (Report). On 13 January 2021, Acesite resubmitted the Full Breach Report.

In an Order dated 21 January 2021, the Commission required Acesite to submit an Updated Report expounding the details of the incident, supplying the lacking information required pursuant to Section 17(D) of the NPC Circular 16-03, and attaching the specified documents to further help with the investigation of the data breach incident.[3] On 01 March 2021, Acesite resubmitted its Full Breach Report.

Issues

The issues in this case are follows:

[2] Full Report on Breach Notification dated 21 March 2018, p. 1-2.
[3] Order dated 21 January 2021, p. 1-2.

1. Whether the matter is a personal data breach; and
2. Whether the matter falls under the mandatory breach notification.

Discussion

I. The matter reported is an availability breach with regard to the loss of the personal data caused by fire.

This Commission finds that the matter reported by Acesite is an availability breach which is one of the natures of a personal data breach. **Section 3(F) of the NPC Circular 16-03 provides:**

> F. "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:
>
> 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. (Emphasis Supplied)

On the other hand, a security incident has a more extensive definition, which is an event or occurrence that affects or tends to affect data protection or may compromise the availability, integrity, and confidentiality of personal data. Further, it includes incidents that would result to a personal data breach, if not for safeguards that have been put in place.[4]

Thus, a data breach is a kind of a security incident considering that it occurs when there is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.[5]

---

[4] Section 3(J) of the NPC Circular 16-03
[5] National Privacy Commission. (n.d.). *Exercising Breach Reporting Procedures.* Retrieved from https://www.privacy.gov.ph/exercising-breach-reporting-procedures/

In this case, the storage and backup storage of the records and files containing personal data of the Hotel's employees and guests is within the premises of the Hotel which was significantly affected by the fire. From the moment that the records and files were destroyed by the fire, the incident becomes an occurrence which affected the data protection and compromised the availability of the personal data of the Hotel's employees and guests.

Considering that the records and files were accidentally destroyed and the personal data of employees and guests were lost, the incident is within the nature of an availability breach resulting from loss and accidental destruction of personal data which cannot be retrieved anymore.

II. The incident does not fall within the scope of the mandatory breach notification requirements.

This Commission finds that this case does not fall under the mandatory breach notification requirements. In order to determine whether an incident falls under the mandatory breach notification requirement, **Section 11 of the NPC Circular 16-03 provides:**

> Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
>
> a. The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

b. There is reason to believe that the information may have been acquired by an unauthorized person; and

c. The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

With the data breach being caused by fire that resulted to the accidental destruction of the personal data involved, there is no reason to believe that the personal data of the Hotel's guests and employees may have been obtained by an unauthorized person and may give rise to real risk of serious harm to the affected data subjects. Although the incident involves personal and sensitive personal information which satisfies the first criteria of the abovementioned section, in order to fall within the scope of the mandatory breach notification requirement, it must also satisfy that the incident may result to unauthorized disclosure or access of personal data and such access may give rise to real risk of serious harm to the affected data subjects.

Thus, with the case only satisfying the first criteria of the Section 11 of the NPC Circular 16-03 and the matter being classified as an availability breach, the notification is not mandatory in this case.

However, in an Order dated 21 January 2021, the Commission through the Complaints and Investigation Division (CID), required Acesite to attach specified documents to further help with the investigation of the incident and submit the lacking information from its initial notification, specifically:

1. Nature of the Breach
   a. Description or nature of the personal data breach;
   b. <u>Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach;</u>
   c. A chronology of the events leading up to the loss of control over personal data;
   d. <u>Approximate number of individuals and/or personal records affected;</u>

e. Description of the likely consequences of the personal data breach on the institution, data subjects and the public;

f. **Description of safeguard in place that would minimize harm or mitigate the impact of the personal data breach;**

- Attach and specify on a report the changes in the data privacy and security policy after the incident particularly on the storage and availability of personal data; Name and contact details of the data protection officer or any other accountable persons.

2. Personal Data Possibly Involved

a. List of the sensitive personal information involved;

b. List of other information involved that may be used to identity fraud;

3. Remedial Measures Taken Subsequent to Suspected 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 or limit the possible harm or negative consequences, damage or distress to those affected by the incident;

d. Actions being taken to inform the data subjects affected by the incident or reasons for any delay in the notification in accordance with Section 21 of the said Circular;

e. The measures being taken to prevent a recurrence of the incident.

- Physical, organizational and technical measures undertaken after the incident, as well as proof thereof. - Where is your backup storage located prior to and after the incident?

In response to the Order, on 01 March 2021, Acesite resubmitted its Report dated 21 March 2018. This Commission notes that Acesite stated in the Report that as part of the mitigating measures and considering that most of the documents were destroyed by the fire, the remaining documents which were beyond retrieval were destroyed through shredding last August 2018. According to Acesite, as a preventive measure against future similar incident, the backup storage of their data will now be isolated in a different location. Acesite also committed to conduct

a Privacy Impact Assessment (PIA) and information asset inventory once the hotel is operational again.[6]

However, the Report resubmitted was the same document initially submitted by Acesite on 29 August 2019 with no new information, additional updates, and attachments required by the previous Order. The resubmitted Report also lacks the updates on the conduct of the PIA and information asset inventory which was initially stated in Acesite's Report and details on the security measures implemented such as details on the isolated backup storage they were planning to implement.

With the resubmission of its initial Report, Acesite has yet to comply with the submission of an Updated Report that consists of the essential information required in the Commission's previous Order dated 21 January 2021.

This Commission then emphasizes that in cases of data breach, including an availability breach, it is within the obligations of the PICs that any or all of their reports are to be made available to the Commission.[7] Moreover, the Commission stresses that the lacking information being required is essential in order for the Commission to be able to identify whether adequate actions were implemented by the PIC to avoid further damage and recurrence of similar incidents, and protect the rights of the data subjects. The Commission's evaluation of such information will not only be beneficial to the data subjects but also to the PICs in improving their personal data breach management policies and procedures.

WHEREFORE, premises considered, Acesite is hereby **ORDERED** to comply with the following within **fifteen (15) days** from receipt of this Resolution:

1. **SUBMIT** its Updated Report with the contents required in the Order dated 21 January 2021; and

[6] Ibid. at p. 2.
[7] Section 22 of the NPC Circular 16-03

2. **SUBMIT** proof and details of the measures taken to address the breach, such as but not limited to, details of implementation of isolated backup storage, information asset inventory, and Privacy Impact Assessment (PIA).

SO ORDERED.

Pasay City, Philippines;
15 April 2021

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

COPY FURNISHED:

JTL
Data Protection Officer

COMPLAINTS AND INVESTIGATION DIVISION
GENERAL RECORDS UNIT
National Privacy Commission