Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: BOMBARDIER TRANSPORTATION (SHARED SERVICES) PHILIPPINES, INC.

NPC BN 21-078

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

RESOLUTION

For Resolution of the Commission is the request of Bombardier Transportation (Shared Services) Philippines, Inc. (Bombardier) for assistance and/or investigation of a suspected personal data breach which allegedly compromised some of its data.

Facts

On 23 April 2021, Bombardier allegedly received a notification about a data exposure.[1] According to an external report from Alstom's data leakage monitoring supplier, fourteen (14) documents from Bombardier Transportation Cebu / Philippines have been exposed via an unprotected FTP server.[2]

On 29 April 2021, an employee from the Human Resources department of Bombardier reported a suspected personal data breach. According to the Incident Report, a laptop used to send files was allegedly infected with Malware or Trojan virus.[3] The file sent was captured in the IP address block for DDT Konstract Inc. Compromised data included the name, age, birthdate, gender, status, and insurance details such as medical insurance coverage of thirteen (13) employees and nine (9) of their dependents.[4]

[1] "Form for Reporting a Suspected Personal Data Breach" dated 29 April 2021, hereinafter referred to as the "Incident Report," p. 2
[2] *Ibid.* at p. 3.
[3] *Ibid at* p. 1.
[4] *Ibid.* at p. 2.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

On 30 April 2021, the Commission received an email from Bombardier requesting for "assistance/investigation on a suspected personal data breach due to a computer virus compromising some Alstom data."[5]

In the same email, Bombardier stated that it implemented the following as part of its remediation measures:

> 1) Even though DDT Konstract is not a company supplier, their IS & Risk compliance Team are now in contact with this supplier to cease processing or forwarding such data accessed/received and delete all the data received.
>
> 2) PIC is asked to shut down laptop used in sending the files while investigation is going on.[6]

On 11 May 2021, Bombardier submitted proof of notification to five (5) data subjects and their dependents.[7]

Discussion

The Commission resolves to deny the request of Bombardier for assistance and/or investigation.

The responsibility of the PIC to investigate a security incident or a personal data breach follows the Accountability Principle provided in the Data Privacy Act:

> Section 21. Principle of Accountability. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

In the exercise of its rule-making power and to flesh out the provision above, the Commission issued NPC Circular No. 16-03 which

[5] Email from Bombardier dated 30 April 2021.
[6] "Form for Reporting a Suspected Personal Data Breach" dated 29 April 2021, hereinafter referred to as the "Incident Report."
[7] Notification and Confirmation emails to five (5) affected data subjects submitted on 11 May 2021.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

recommends, among others, the establishment of policies and procedures by PICs for the conduct of investigations and the full assessment and evaluation of a security incident or a personal data breach.

In case of a security incident or a personal data breach, a PIC is expected to conduct an investigation as part of its policies and procedures. Section 8 of NPC Circular No. 16-03 provides that:

> **SECTION 8. *Policies and Procedures***. The personal information controller or personal information processor shall implement policies and procedures for guidance of its data breach response team and other personnel in the event of a security incident. These may include:
>
> A. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
>
> B. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;
>
> C. Conduct of a preliminary assessment for purpose of:
>   1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
>   2. Determining the need for notification of law enforcement or external expertise; and
>   3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
>
> D. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;
>
> E. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

> **F. Conduct of investigations that will evaluate fully the security incident or personal data breach;**
>
> G. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and
>
> H. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.[8]

The PIC, upon knowledge of or when there is reasonable belief that a personal data breach requiring notification has occurred, is required to notify the Commission and the affected data subjects within seventy-two (72) hours:[9]

> **SECTION 17. *Notification of the Commission*.** The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> A. *When Notification Should be Done*. **The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.**
>
> xxx
>
> **SECTION 18. *Notification of Data Subjects*.** The personal information controller shall notify the data subjects affected by a personal data breach, subject to the following procedures:
>
> A. *When should notification be done*. **The data subjects shall be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.** The notification may be made on the basis of

[8] Section 8, NPC Circular No. 16-03, "Personal Data Breach Management."
[9] Sections 17(A) and 18(A), NPC Circular No. 16-03.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

> available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects. It shall be undertaken in a manner that would allow data subjects to take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be supplemented with additional information at a later stage on the basis of further investigation.

Aside from the initial notification, the PIC should submit a full breach report in accordance with the requirements of NPC Circular No. 16-03:

> **SECTION 17. *Notification of the Commission*.** The personal information controller shall notify the Commission of a personal data breach subject to the following procedures:
>
> xxx
>
> C. 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.
>
> D. *Content of Notification*. 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
> 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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

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.

E. *Form.* Notification shall be in the form of a report, whether written or electronic, containing the required contents of notification: *Provided*, that the report shall also include the name and contact details of the data protection officer and a designated representative of the personal information controller: *Provided further*, that, where applicable, the manner of notification of the data subjects shall also be included in the report. Where notification is transmitted by electronic mail, the personal information controller shall ensure the secure transmission thereof. Upon receipt of the notification, the Commission shall send a confirmation to the personal information controller. A report is not deemed filed without such confirmation. Where the notification is through a written report, the received copy retained by the personal information controller shall constitute proof of such confirmation.[10]

A PIC should have processes and procedures in place to prevent security incidents and personal data breaches. The DPA and its issuances provide that a PIC should have protocols for investigating a breach, notification of the Commission and the affected data subjects, and for implementation of remediation measures to address the situation and to prevent the incident from recurring.

[10] Section 17(C), (D) and (E), NPC Circular No. 16-03.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

The Commission notes from Bombardier's request that it has not even conducted its own investigation and wants to merely rely on the Commission to conduct it for them. The Commission stresses the responsibility of a PIC to conduct its own investigation on any security incident or personal data breach in their systems, its responsibility to notify all the affected data subjects and its responsibility to submit a Full Breach Report within the time prescribed in NPC Circular No. 16-03. As of this date, Bombardier has neither submitted its full breach report nor requested for an extension of time to file the same. Moreover, from the documents submitted, only five (5) of the thirteen (13) affected employees have been notified of the incident.

WHEREFORE, all premises considered, the Commission hereby **DENIES** the request of Bombardier Transportation (Shared Services) Philippines, Inc. for assistance and investigation and hereby **ORDERS** Bombardier to **NOTIFY** the affected data subjects, and to **SUBMIT** the following **within fifteen (15) days** from receipt of this Resolution:

1. Privacy Policy, particularly its policies and processes relating to breach response;

2. A Full Breach Report; and

3. Proof of notification to the eight (8) remaining affected data subjects.

SO ORDERED.

City of Pasay, Philippines;
01 June 2021.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY D. NAGA
Deputy Privacy Commissioner

COPY FURNISHED:

MDC
HR Business Partner – SSC Cebu
Bombardier Transportation (Shared Services)
Philippines, Inc. (Alstom)

COMPLIANCE AND MONITORING DIVISION
GENERAL RECORDS UNIT
National Privacy Commission

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: http://privacy.gov.ph Email Address: info@privacy.gov.ph