Republic of the Philippines
NATIONAL PRIVACY COMMISSION

IN RE: MOVIE AND TELEEVISION REVIEW AND CLASSIFICATION BOARD

CID BN NO. 17-010

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

ORDER

AGUIRRE, D.P.C.:

This Order refers to a letter submitted by the Movie and Television Review and Classification Board (MTRCB) dated 04 February 2021. The letter contains a comprehensive report on its compliance with the previous orders of the Commission.

The Facts

On 20 September 2017, the MTRCB notified the Commission of a cybersecurity incident which led to a breach of the data stored in its system.[1]

The breach was estimated to have occurred between the first week of September 2017 until its discovery on 19 September 2017.[2] Upon initial assessment, two (2) out of the three (3) backup servers were compromised. Consequently, the files in the affected servers (Servers 1 and 2) were maliciously encrypted and renamed with a file extension (.arena).

The personal information affected includes publicity materials, and the backup copies of MTRCB's database for Electronic New Government Accounting Management System (e-NGAS). This database contains the following information: (1) MTRCB Members of the Board, Employee, and Organic Staff Names and Tax Identification Numbers (TIN); (2) Contracted Vendors/Suppliers Business Name

[1] Records at pp. 1-3.
[2] *Ibid.*

and TIN; (3) Monetary Remittances through MTRCB Payroll and Vendor Payments; and (4) List of MTRCB's Property Plant Equipment.[3]

According to MTRCB's data breach notification, the personal data of five hundred seventy-three (573) data subjects were affected. These include one hundred ninety-three (193) current and former employees and board members, as well as three hundred eighty (380) active and former suppliers, contractual employees, and consultants of MTRCB.[4]

Shortly after its breach notification report, on 21 September 2017, MTRCB sent a letter[5] to the Commission requesting for the postponement of the notification of the data subjects for twenty (20) days. MTRCB also reported that since the discovery of the breach, it was in close contact with the proper government agencies such as the Department of Information and Communications Technology ("DICT") and the Philippine National Police ("PNP") for the expeditious resolution of the case.[6]

On 5 October 2017, the Commission sent an e-mail[7] to MTRCB in response to the latter's data breach incident report. The Commission required MTRCB to submit a full breach report following the requirements set forth in NPC Circular No. 16-03 on Data Breach Management within five (5) days from receipt of the e-mail.[8]

On 10 October 2017, MTRCB submitted its full breach report along with a request for exemption from notification of data subjects.[9] In its full breach report, MTRCB outlined its proposed remedial measures including an application for Vulnerability and Penetration Test (VAPT) with the DICT, installation of new antivirus software, and reformatting of the servers to prevent the spread of the virus to workstations.[10]

---

[3] *Id.* at p.1.
[4] I*d.* at p.12.
[5] Re: Request for Postponement of Notification for Data Subjects affected by Data Breach at pp. 4-5.
[6] *Id* at p. 5.
[7] *Id.* at p. 10.
[8] *Id.*
[9] *Id*. at pp. 11-14.
[10] *Id.*

As to the actions taken to inform the data subjects, the MTRCB explained that upon close coordination with the DICT and PNP Anti Cyber Crime Group, both agencies were not able to provide information that the encrypted data were passed on or at risk of being uploaded on the internet for exploitation. In support of its request for exemption from notification of the data subjects, MTRCB also argued that ransomware attacks only encrypt data for extortion particularly by demanding a ransom to decrypt the infected files.[11]

On 31 January 2018, the Commission issued a Compliance Order[12] against MTRCB directing the latter to do the following:

1. Appoint or designate a Data Protection Officer within one (1) month from the receipt of the Order;

2. Create a Privacy Management Program based on risk assessment within three (3) months from receipt of Order;

3. Implement appropriate organizational, physical, and technical security measures in accordance with the provisions of NPC Circular No. 16-03, on Security of Personal Data in Government Agencies and submit a progress report within six (6) months from receipt;

4. To cause the conduct of an independent security audit of all its personal data processing systems including those hosted by service providers, within six (6) months from receipt of Order, and;

5. Notify the data subjects affected in accordance with NPC Circular No. 16-03 within fifteen (15) days from receipt of the Order.[13]

On 08 March 2018, MTRCB, in a letter, acknowledged the receipt of the Compliance Order. However, it reiterated its request to be exempted from notifying the data subjects affected by the breach.[14] MTRCB

---

[11] *Id*. at p. 14.
[12] *Id.* Compliance Order at pp. 24-26.
[13] *Id*. at p.25.
[14] Letter from MTRCB dated 7 March 2018.

averred that the encoded employee numbers of the data subjects contained in the compromised backup e-NGAS database were only dummy data and thus could not be used for malicious purposes. According to MTRCB, the data was only made up using either a TIN number or a combination of made-up number and TIN number.[15]

In case the exemption was not feasible, MTRCB requested for a sixty (60)-day extension period from the date of the letter for it to determine the specific number of data subjects affected. It also requested alternative means of notification of the data subjects.[16]

On 06 January 2021, the Legal and Enforcement Office ("LEO") sent a Compliance Letter[17] to MTRCB instructing it to submit a comprehensive report of its implementation and compliance with the order of the Commission dated 31 January 2018.

In a letter dated 04 February 2021, received by LEO on 17 February 2021, MTRCB submitted its comprehensive report[18] on its compliance with the previous orders of the Commission. MTRCB reported that it has already created a Privacy Management Program and has implemented its security measures in accordance with NPC Circular No. 16-01 or the Security of Personal Data in Government Agencies. As to the conduct of an independent security audit, MTRCB said that it was already processing the necessary documentary requirements for engaging the services of a security audit provider. As to the notification of data subjects, MTRCB reiterated its request for exemption and alternate means of notification to the affected data subjects, which was not responded to by the Commission.[19]

Discussion

The Commission notes the following actions of the MTRCB to comply with the 31 January 2018 Compliance Order:

---

[15] *Id.*
[16] *Id.*
[17] Compliance Letter Re: Compliance Order dated 31 January 2018.
[18] Comprehensive report of MTRCB's implementation of and compliance with the NPC Order dated 31 January 2018.
[19] *Id.*

(1) Appointment of a Data Protection Officer;[20]

(2) Creation of a Privacy Management Program (PMP) based on risk assessment;[21]

(3) Implementation of appropriate organizational, physical and technical security measures in accordance with the provisions of NPC Circular No. 16-01 on Security of Personal Data in Government Agencies and submission of a progress report within six (6) months from receipt of the order.[22]

The Commission notes the MTRCB's submission of its PMP, Privacy Impact Assessment, updates, and reports. However, MTRCB has yet to comply with the following directives: (1) Conduct of an independent security audit of all its personal data processing systems including those hosted by service providers; and (2) Notification of data subjects.

In a letter dated 07 March 2018, MTRCB requested to be exempted from notifying the data subjects. If the extension is not feasible, it requested for a sixty (60)-day extension period.

At the outset, it should be emphasized that notification of data subjects of a personal data breach is the general rule and exemptions are allowed only under specific circumstances. Section 18(A) of NPC Circular No. 16-03, provides the rule:

> **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 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

[20] Email from the Compliance and Monitoring Division dated 3 February 2021.
[21] Annex A, Letter dated 4 February 2021.
[22] Letter dated 4 February 2021.

> 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. **(Emphasis supplied)** [23]

The purpose of the requirement to notify data subjects of a breach incident is for them to take the necessary precautions or such other measures to protect themselves against possible effects of the breach. Personal information controllers (PICs) are likewise required to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.[24]

Section 18(B) of NPC Circular No. 16-03 provides for the criteria of exemption, thus:

> **If it is not reasonably possible to notify the data subjects within the prescribed period, the personal information controller shall request the Commission for an exemption from the notification requirement**, or the postponement of the notification**. A personal information controller may be exempted from the notification requirement where the Commission determines that such notification would not be in the public interest or in the interest of the affected data subjects.** The Commission may authorize the postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach, taking into account circumstances provided in Section 13 of this Circular, and other risks posed by the personal data breach.[25]

As of date, MTRCB has yet to submit proof of notification of the affected data subjects. If indeed MTRCB deemed it necessary to notify the data subjects and asked the Commission in good faith for an extension period of sixty (60) days, then it should have proceeded to notify the data subjects after the lapse of the sixty (60)-day period.

As indicated in the breach notification report, the personal data of at least five hundred seventy-three (573) individuals were compromised. The affected data involves sensitive personal information or any other information that may be used to enable identity fraud. Given this

---

[23] NPC Circular 16-03, Personal Data Breach Management. Dated 15 December 2016. Emphasis supplied.
[24] *Ibid.*
[25] Emphasis supplied.

situation, the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

Even after multiple requests of postponement of or exemption from notification of data subjects, the Commission, on 31 January 2018, issued a Compliance Order to MTRCB which included, among others, an order to proceed with the notification of data subjects. Such Compliance Order is proof that the Commission has not found any ground to dispense with the notification requirement and MTRCB failed to prove that it was indeed entitled to exemption.

As regards the independent security audit, MTRCB stated in its report that it is still preparing to conduct it on all its personal data processing systems including those hosted by service providers. The Commission deems it reasonable to require compliance with this within three (3) months from receipt of this Resolution.

WHEREFORE, premises considered, the Commission **ORDERS** the Movie and Television Review and Classification Board to comply with the following:

(1) **NOTIFY** the data subjects affected by the breach incident **within fifteen (15) days** from receipt of this Order;

(2) **SUBMIT** proof of notification that ensures all data subjects were made aware of the breach, **within fifteen (15) days** from receipt of this Order; and

(3) **SUBMIT** the results of the independent security audit **within three (3) months** from receipt of this Order.

SO ORDERED.

City of Pasay, Philippines.
15 April 2021.

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:

MLN
Officer-in-Charge
Office of the Executive Director
Movie and Television Review and Classification Board

COMPLAINTS AND INVESTIGATION DIVISION
ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission