IN RE: POWERVISION EAP, INC. **NPC BN 21-097**

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

ORDER

Before this Commission is a request for extension to submit documents filed by PowerVision EAP, Inc. (PowerVision) dated 04 January 2022, in relation to a phishing incident of its email account. PowerVision also requests guidance from the Commission on a possible exemption from data subject notification.

Facts

In the Initial Report sent on 23 May 2021 (Initial Report), PowerVision reported a security incident that happened on 20 May 2021 wherein the password of its administrative email account (help@powervisioneap.com) was cracked and subsequently used to send phishing emails to recipients.[1]

Particularly, emails were sent using the administrative email account containing an audio file that would require the person accessing it to input the Outlook email and password. The Initial Report also contained a request for extension of time of fifteen (15) days to file the Full Breach Report. [2]

PowerVision subsequently submitted a Full Report dated 07 June 2021 (Full Report). In the cover letter of the Full Report, PowerVision related that it had analyzed twenty-five thousand eight hundred eighty-seven (25,887) emails, over which four hundred eighty-two (482) emails contained personal data.[3] The sensitive personal information contained in

[1] Initial Report dated 23 May 2021 filed by PowerVision EAP, Inc.
[2] Id.
[3] Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

the emails included "the mental or emotional health condition of the data subject and possibly some isolated number of government identifiers."[4]

As part of its efforts to address the phishing incident, PowerVision changed the password of their administrative email account, and temporarily deactivated it.[5] Notifications were sent to the three hundred eighty-seven (387) recipients of the phishing email and PowerVision's client points-of-contact to inform them about the incident, requiring them to change their password, and perform anti-virus scans on their device.[6] On 24 May 2021, multi-factor authentication was required to access all PowerVision-issued email accounts. It also claimed that after investigation, the intruder did not download any emails from the account.[7]

In its cover letter containing the Full Report, PowerVision requested guidance from the Commission on whether an exemption from notifying its data subjects was allowable "since there was no sensitive personal data acquired by the intruder and that the possible emotional and mental effect which may unnecessarily burden the data subject is not proportionate to the minimal possible risk."[8]

In an Order dated 08 June 2021 (Order), the Compliance and Monitoring Division (CMD) of the Commission ordered PowerVision to submit the following documents within a period of five (5) days from receipt, *to quote*:

> **WHEREFORE**, premises considered, **the PowerVision EAP Inc.** is **ORDERED**: **TO SUBMIT** the following documents:
>
> 1. Lacking details on the full breach report based on the provisions of NPC Circular 16-03:
>
> a. Description how the breach occurred and the vulnerability of the data processing system that allowed the breach.
> b. Chronology of events.

[4] Full Report dated 07 June 2021 filed by PowerVision EAP, Inc.
[5] Id.
[6] Id.
[7] Id.
[8] Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

c. Description of the likely consequences of the personal data breach. Provide how will the incident affect both the PIC and its data subjects.
d. Measures to secure/recover personal data.
e. Actions to mitigate harm.
f. Actions taken to inform data subjects. Provide the actual manner of notification. Include the assistance extended to data subjects, if there is any.
g. Measures being taken to prevent a recurrence of the incident. Provide the portion of the actual or proposed orientation materials addressing the vulnerability identified.

2. Security Incident Management Policy;
3. Privacy Manual;
4. Copy of the data subject notification; and
5. Policies relating to human Resource security, cryptography, access control, communications security, and compliance

POWERVISION EAP INC. is hereby given a period of five (5) days from receipt hereof to submit its compliance through email at breach@privacy.gov.ph.

SO ORDERED.[9]

PowerVision received the Order on 03 January 2022. Through an email on 04 January 2022, its Data Protection Officer (DPO) requested an extension until 28 January 2022 to submit the documents in the CMD's Order since: 1) the DPO was currently out of the country and had no access to the files needed; and 2) the DPO tested positive for Covid-19 and there was a possibility of delay in returning to the Philippines.[10]

Issue

I. Whether to grant the request for extension until 28 January 2022 to submit the documents outlined in the Order dated 08 June 2021.

II. Whether to grant the request for exemption from data subject notification.

[9] Order dated 08 June 2021.
[10] Email Request dated 04 January 2022 of PowerVision EAP, Inc.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Discussion

The Commission grants PowerVision's request for an extension until 28 January 2022 to submit the documents outlined in the CMD's Order dated 08 June 2021. It denies its request for exemption from data subject notification.

A Personal Information Controller has the obligation to ensure the accessibility of documents and information related to the personal data breach.

PowerVision, as the Personal Information Controller (PIC), is expected to comply with the periods stated in NPC Circular No. 16-03 (Personal Data Breach Management)[11] and with the corresponding orders of the Commission. Particularly, Section 17(C) of NPC Circular No. 16-03 requires the submission of a Full Breach Report within five (5) days from initial notification, "unless the personal information controller is granted additional time by the Commission to comply."[12]

Further, Section 18(A) of the same Circular states:

> **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 take the necessary precautions or other measures to protect themselves against the possible effects of the breach. It may be

[11] *see* NPC Circular No. 16-03, Section 17(A) and (C); Section 18(A).
[12] NPC Circular No. 16-03, Section 17(C).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> supplemented with additional information at a later stage on the basis of further investigation.[13]

Considering the abovementioned provisions, the Full Breach Report must be submitted within five (5) days from filing the Initial Report.[14] While, the notification to the affected data subjects must be made based on available information within the 72-hour period.[15]

PowerVision now requests an extension to submit documents given that they are allegedly inaccessible due to the DPO's physical location and health condition.[16]

The Commission notes that in PowerVision's cover letter containing the Full Report, it stated that due to the pandemic, "counselling sessions are made through online platform or via audio calls."[17] As a company that relies on technology, particularly during the pandemic, it would also be reasonable to infer that the documents are digitized and accessible. Thus, the files or documents needed would be accessible regardless of the physical location or health condition of the DPO.

Further, Section 5 of NPC Circular No. 16-03 requires a data breach response team as part of the guidelines for personal data breach management, *to quote:*

> **SECTION 5.** ***Data Breach Response Team.*** A personal information controller or personal information processor shall constitute a data breach response team, which shall have at least one (1) member with the authority to make immediate decisions regarding critical action, if necessary. **The team may include the Data Protection Officer.**
>
> The team shall be responsible for the following:
>
> A. Implementation of the security incident management policy of the personal information controller or personal information processor;

[13] Section 18(A) of the NPC Circular No. 16-03.
[14] Section 17(C) of the NPC Circular No. 16-03.
[15] Section 18(A) of the NPC Circular No. 16-03.
[16] Id.
[17] Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> B. Management of security incidents and personal data breaches; and
>
> C. Compliance by the personal information controller or personal information processor with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.
>
> The team must be ready to assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage, and comply with reporting requirements.
>
> **The functions of the Data Breach Response Team may be outsourced. Such outsourcing shall not reduce the requirements found in the Act, the IRR or related issuance. The Data Protection Officer shall remain accountable for compliance with applicable laws and regulations.**[18] (Emphases supplied)

As the quoted provision shows, the responsibility for complying with NPC Circular No. 16-03 does not rest solely with the DPO. The PIC should have a data breach response team in place to handle proceedings related to data breaches. In this case, even though PowerVision's DPO is abroad and has contracted Covid-19, members of PowerVision's data breach response team should be available to comply with the CMD's Order.

Further, the Commission once again reminds PICs that the prompt compliance with the Commission's orders is within their responsibilities and obligations in cases of data breach, especially if the incident involves sensitive personal information[19] and the affected data subjects are more than one hundred (100) individuals.[20]

The Commission has the authority to grant the PIC an additional period to comply with the submission of documents.

[18] Section 5 of the NPC Circular No. 16-03.
[19] Section 11(A) of the NPC Circular No. 16-03 .
[20] Section 13(B) of the NPC Circular No. 16-03.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

Nevertheless, in the interest of substantial justice and due process, the Commission now exercises its authority to grant PowerVision's request for extension. In granting PowerVision's request for extension, the Commission applies liberality and shall allow the PIC to submit the additional documents based on its requested period, *i.e.*, 28 January 2022.

The Commission expects that PowerVision will comply in good faith with the period requested. As previously ruled by the Commission: "A PIC is expected to comply with the Commission's Order within the period that the PIC itself requested from the Commission."[21]

The PIC must notify data subjects in cases which fall under the mandatory breach notification requirement.

In the cover letter attaching its Full Report, PowerVision requested guidance from the Commission on whether it may be exempted from notifying the affected data subjects.[22] It claims that "there was no sensitive personal data acquired by the intruder and that the possible emotional and mental effect which may unnecessarily burden the data subject is not proportionate to the minimal possible risk."[23] This request for guidance shall be treated by the Commission as a request for exemption from data subject notification.

The Commission finds that the reported breach falls under the mandatory breach notification requirement, and notification is crucial in order to reduce the risks and possible harm to the affected data subjects. Section 11 of NPC Circular No. 16-03 provides:

> **SECTION 11.** ***When notification is required.*** 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:

[21] NPC BN 20-129 In re: DB Schenker Global Service Asia Pacific Inc.. Resolution dated 02 September 2021. At page 6.
[22] Cover Letter dated 07 June 2021 of PowerVision EAP, Inc.
[23] Id.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> 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.**[24] (Emphases supplied)

Further, Section 13(B) and (C) of NPC Circular No. 16-03, in relation to Section 11 of the same Circular provides:

> **SECTION 13.** ***Determination of the Need to Notify***. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:
>
> xxx
>
> B. At least one hundred (100) individuals;
>
> C. Information required by applicable laws or rules to be confidential;[25]

Here, PowerVision itself identified that the personal data breach involved sensitive personal information since four hundred and eighty-two (482) emails in the administrative email account contained "the mental or emotional health condition of the data subject and possibly some isolated

[24] Section 11 of the NPC Circular No. 16-03.
[25] Section 13(B) and (C) of the NPC Circular No. 16-03

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

number of government identifiers".[26] The number of data subjects is more than one hundred (100) since three hundred eighty-seven (387) people were recipients of the phishing email. The two circumstances combined require PowerVision to notify the affected data subjects.[27]

In this case, there are also insufficient grounds for the exemption of notification of affected data subjects. Section 18(B) of NPC Circular No. 16-03 provides for situations that may exempt a PIC from notifying data subjects, *to quote:*

> **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:
>
> xxx
>
> B. *Exemption or Postponement of Notification*. 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.[28]

Section 19 of NPC Circular No. 16-03 further provides:

> **SECTION 19.** ***Exemption from Notification Requirements***. The following additional factors shall be considered in determining whether the Commission may exempt a personal information controller from notification:
>
> A. Security measures that have been implemented and applied to the personal data at the time the personal data breach was reasonably believed to have occurred, including measures that would prevent use of the personal data by any person not authorized to access it;

---

[26] Full Report dated 07 June 2021 filed by PowerVision EAP, Inc.
[27] Id.
[28] Section 18(B) of the NPC Circular No. 16-03.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

> B. Subsequent measures that have been taken by the personal information controller or personal information processor to ensure that the risk of harm or negative consequence to the data subjects will not materialize;
>
> C. Age or legal capacity of affected data subjects: *Provided*, that in the case of minors or other individuals without legal capacity, notification may be done through their legal representatives.
>
> In evaluating if notification is unwarranted, the Commission may take into account the compliance by the personal information controller with the law and existence of good faith in the acquisition of personal data.[29]

The Commission notes that the type of sensitive personal information involved may be used to enable identity fraud. Also, the breach of the data subjects' patient records (*i.e.*- the mental or emotional health conditions) may expose them to harassment, discrimination, or other risks of real and serious harm. Further, PowerVision failed to provide actual proof of the security measures it has implemented during the breach and subsequent measures it has implemented for the risk of harm or negative consequence to the affected data subjects will not materialize. The Commission finds that PowerVision has not sufficiently shown that notification is not reasonably possible, and given the circumstances, an exemption from notification would not be in the best interest of affected data subjects.

Considering the type of personal information involved and the number of affected data subjects, the Commission deems it wise for PowerVision to promptly notify the affected data subjects. This is in order to allow them to take the necessary precautions or other measures to protect themselves against the potential harm or negative consequences resulting from the breach.[30]

WHEREFORE, premises considered, PowerVision EAP, Inc.'s (PowerVision) request for an extension to submit the documents enumerated in the Compliance and Monitoring Division's Order dated 08 June 2021, is hereby **GRANTED.** PowerVision is **ORDERED** to submit the required documents as stated in the CMD Order dated 08 June 2021 until **28 January 2022, namely:**

---

[29] Section 19 of the NPC Circular No. 16-03.
[30] *See* NPC Circular No. 16-03, Section 18(A).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

1. Details on the full breach report based on the provisions of NPC Circular 16-03:

    a. Description how the breach occurred and the vulnerability of the data processing system that allowed the breach.
    b. Chronology of events.
    c. Description of the likely consequences of the personal data breach. Provide how will the incident affect both the PIC and its data subjects.
    d. Measures to secure/recover personal data.
    e. Actions to mitigate harm.
    f. Actions taken to inform data subjects. Provide the actual manner of notification. Include the assistance extended to data subjects, if there is any.
    g. Measures being taken to prevent a recurrence of the incident. Provide the portion of the actual or proposed orientation materials addressing the vulnerability identified.

2. Security Incident Management Policy;
3. Privacy Manual;
4. Copy of the data subject notification; and
5. Policies relating to human Resource security, cryptography, access control, communications security, and compliance

PowerVision is further **ORDERED** to notify the affected data subjects, and submit proof of notification thereof.

SO ORDERED.

City of Pasay, Philippines.
27 January 2022.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

I CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Copy furnished:

RVN.
Data Protection Officer of PowerVision

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

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228