IN RE: PHILIPPINE STATISTICS AUTHORITY NPC BN 23-239

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

ORDER

Before the Commission is the request for postponement and use of alternative means of notification filed by the Philippine Statistics Authority (PSA) through the Data Breach Notification Management System (DBNMS) dated 10 October 2023.[1]

In its initial report in the DBNMS, it was stated that on 07 October 2023, a PSA employee came across a post by Diablox-Phantom #01 in Facebook.[2] The said Facebook post was captioned, "Philippines Statistics Authority | PSA Data Leak: Sample Record Database Full 42Billion."[3] "Mas Magandang mamatay sa digmaan kesa tanggapin ang maling pamumuno ng bayan, kung panaginip lamang ang umasa sa pagunlad ng bayan, managinip tayo hanggang sa kamatayan MMM2k23."[4]

On 08 October 2023, the Facebook page of Diablox-Phantom #01 was no longer active, however, there is a newly created account under the name Diablox-Phantom #02 with shared identical links.[5] Also, PSA stated that it discovered that when the posted Uniform Resource Locator (URL) is clicked, it redirects to phishing and clickbait websites.[6] In addition, it is also reported that there are social media sites that posted the same statements and links, such as Deep Web Konek, ES, and Philippine I.T. Security Forums.[7]

---

[1] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[6] *Id.*
[7] *Id.*

Moreover, on 09 October 2023, PSA's Information Technology (IT) team identified a suspicious file stored in its Network Attached Storage (NAS).[8] PSA stated that based on its logs, the file was uploaded to the storage on 15 September 2023 and that on 26 September 2023, there were downloads in the server not authorized by any PSA personnel.[9] In the initial report, PSA stated that there are "possible files containing responses pertaining to demographic information of survey respondents."[10]

To address the breach, PSA stated that it took offline its NAS, Management Information System (MIS), and FilePinas to prevent unauthorized access. It also activated its Data Breach Response Team (DBRT), conducted an investigation to identify the root cause of the incident for any weaknesses in the MIS, and performed Vulnerability Assessment and Penetration Testing (VAPT) to determine the vulnerabilities in its system.[11]

Further, PSA requested for the postponement to notification of affected data subjects, stating that the "affected data subjects [are] yet to be identified" as its justification for its request[12]

On 20 October 2023, the Commission issued a Minute Resolution ordering PSA to submit proof to substantiate its request for postponement to notify the affected data subjects:

> Pursuant to Section 17 (D) of NPC Circular 16-03 (Personal Data Breach Management), the Commission may require additional information, if necessary, for the proper resolution of the request for postponement to notify the affected data subjects
>
> **WHEREFORE**, premises considered, the Commission hereby **ORDERS** Philippine Statistics Authority to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for postponement to notify the affected data subjects.

---

[8] *Id.*
[9] *In re: Philippine Statistics Authority* NPC BN 23-239, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (10 October 2023).
[10] *Id.*
[11] *Id.*
[12] *Id.*

> Should the Philippine Statistics Authority fail to provide the foregoing, this matter shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED**.[13]

On 31 October 2023, PSA submitted its Compliance to the Minute Resolution.[14]

In its Compliance, PSA reiterated that "request for postponement of notification to data subjects was made as it was not possible to identify the number of data subjects within seventy-two (72) hours from the discovery of the security incident."[15] Further, PSA was able to identify the affected system and the affected group of data subjects, seventy-two (72) hours after the discovery of the incident.[16] It was identified that the affected group of data subjects belonged to the Community Based Monitoring System (CBMS).[17]

For context, the CBMS contains information obtained by a team composed of Enumerators, Team Supervisors, Area Supervisors, Head Area Supervisors, and PSA Provincial and Regional Focal persons collected from the head of households.[18]

As to the number of affected data subjects, PSA declared that there are approximately ninety-three thousand seven hundred sixty (93,760) affected data subjects by the mean of averaging the members per household, thus:

> At the moment, approximately 23,440 households are affected by the incident. On the average a household is composed of four members. Thus, approximately 93,760 individuals are affected. There is also an estimated 49,000 Enumerators, Team Supervisors Area Supervisors, Head Area Supervisors and PSA Provincial

---

[13] *In re: Philippine Statistics Authority* NPC BN 23-239, Minute Resolution dated 21 October 2023, at p. 1.
[14] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.
[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.

> and Regional Focal persons whose personal information are affected.[19]

Additionally, according to PSA, it intends to notify the affected data subjects through the head of the households since the information was collected through them.[20] It will also hire additional manpower to conduct house-to-house delivery of notification.[21] However, considering the number of data subjects, it stated that it needs to "employ also additional means to reach the [data subjects] in the most expedient time."[22] Thus, PSA requests for the use of alternative means of notifying the affected data subjects.[23]

Subsequently, PSA claimed that it will train personnel who will conduct the notification through the heads of the households.[24] Further, the said manpower personnel tasked to conduct the notifications "will be trained to use a secure means of communication, proper identification of the data subject to be notified and will be required to submit an Oath of Data Privacy."[25]

Lastly, PSA stated that it will set up a help desk or a portal where affected data subjects can obtain more detailed information with regard to the incident.[26] Its Legal Service (LS) and the Data Protection and Security Unit (DPSU) will oversee the proposed procedure of data subject notification.[27] Additionally, the LS and DPSU of PSA will train its personnel and will conduct random audits to ensure its compliance with NPC Circular No. 16-03 (Personal Data Breach Management).[28]

The Commission denies PSA's request for postponement of data subject notification and request for use of alternative means of data subject notification.

---

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023.
[27] *Id.*
[28] *Id.*

Section 18 (B) of NPC Circular No. 16-03 provides:

> *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. **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.**[29] (Emphasis supplied)

To reiterate, PSA's justification for its request for postponement is that the affected data subjects are yet to be identified. However, such justification does not fall within the circumstances when the Commission may authorize the postponement of data subject notification. In this case, notifying the affected data subjects will not hinder the progress of a criminal investigation. Thus, PSA's request for postponement of data subject notification does not fall within the ambit of the above-stated provision.

Additionally, PSA requests for the use of alternative means of notification. According to PSA, it "intends to notify the data subjects through the head of household as the information was collected through them."[30]

Section 18 (D) of NPC Circular No. 16-03 states that:

> D. Form. **Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic.** The personal information controller shall take the necessary steps to ensure the proper identity of the data subject being notified, and to safeguard against further unnecessary disclosure of personal data.
> **The personal information controller shall establish all reasonable mechanisms to ensure that all affected data subjects**

[29] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(B) (15 December 2016) (NPC Circular 16-03).
[30] Compliance (With Request for Alternative Mode of Notification) by Philippine Statistics Authority dated 31 October 2023

> **are made aware of the breach**: Provided, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification, such as through public communication or any similar measure through which the data subjects are informed in an equally effective manner: Provided further, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach. (Emphasis supplied)

The Commission emphasizes that the notification to the affected data subjects must be done individually.[31] Also, the Commission stresses that PSA has the obligation to establish all reasonable mechanisms to ensure that all affected data subjects are made aware of the breach.[32] PSA, as the PIC, must not automatically resort to the use of alternative means of notification without exhausting reasonable mechanisms to notify all data subjects affected by the breach.

In seeking the approval of the Commission to use alternative means of data subject notification, PSA failed to justify that "individual notification is not possible or would require disproportionate effort" as stated in Section 18(D) of NPC Circular No. 16-03. Nothing in its submission proves that individual notification is not possible or would need disproportionate effort to notify the affected data subjects.

Further, the Commission finds that notification of the head of the household alone is insufficient. It bears stressing that notification of the head of the household is not tantamount to notification to the affected members of the household. Notwithstanding that the information was collected through the head of the household, data subjects who are members of the household whose personal data was affected by the breach, must also be notified of such incident in order to allow them to take precautions against the likelihood of harm or risk that the incident might cause.[33]

Moreover, the Commission underscores the necessity for PICs to identify the affected data subjects and personal data involved in

---

[31] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 18(D) (15 December 2016) (NPC Circular 16-03).
[32] *Id.*
[33] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, § 13 (15 December 2016) (NPC Circular 16-03).

breach incidents. In this case, it must be noted that individuals whose personal data are involved, such as sensitive personal information as defined in Section 3(l) of the DPA, and any other information that may be used to enable identity fraud as provided in Section 11(A) of the NPC Circular No. 16-03 are considered the affected data subjects. Thus, individuals whose personal data falls under the definition of the aforementioned provisions must be individually notified.

Furthermore, in establishing all mechanisms to ensure that affected data subjects are made aware of the breach, PSA may carry out the individual notification through sending the data subject notification of members of the household whose personal data is affected by the breach to the head of the household. PSA must provide an individual data subject notification to the members of the household affected by the breach through the head of the household.

In terms of notification to the Commission, although there is no requirement under Section 17(D) of NPC Circular No. 16-03 to determine the precise number of affected data subjects, PICs must employ due diligence and effort in determining the number of affected data subjects to ensure accurate notification to the Commission, especially if the PIC has the information to already determine the precise number of affected data subjects.

WHEREFORE, premises considered, the Commission **DENIES** Philippine Statistics Authority's request for postponement of notification to the affected data subjects and request for the use of alternative means of data subject notification.

The Philippine Statistics Authority is hereby directed to **NOTIFY** all affected data subjects individually through the head of the household.

Further, the Commission **DIRECTS** the Compliance and Monitoring Division (CMD) to issue appropriate orders necessary to evaluate and monitor the completeness of the Philippine Statistics Authority's data breach notification and assess its breach management pursuant to NPC Circular No. 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
13 November 2023.

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

WE CONCUR:

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

EPA
Data Protection Officer
PHILIPPINE STATISTICS AUTHORITY

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