IN RE: PHILIPPINE NATIONAL POLICE **NPC BN 23-110**

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

ORDER

Before the Commission is Philippine National Police (PNP)'s request for alternative means of notification to the affected data subjects dated 26 April 2023 submitted through the Data Breach Notification Management System (DBNMS).

According to PNP's initial report, on 18 April 2018, JF published an online article pertaining to a massive breach of data involving Philippine Police employees.[1] Thereafter, on 24 April 2023, the PNP Recruitment and Selection Service (PRSS) confirmed through cross-matching the screenshots of the sample data provided by the National Privacy Commission (Commission).[2] It was confirmed that seven out of ten of the samples were stored in the PNP's Comprehensive Online Recruitment Encrypting System (CORES) storage server.[3]

Further, PNP claimed that as of 25 April 2023, the seven affected data subjects were already notified through electronic mail.[4] PNP also stated, "[t]here is no indication yet that the said documents were downloaded pending the analysis of the logs provided to [National Privacy Commission] and [PNP Anti-Cybercrime Group]."[5]

Additionally, PNP stated that its justification for its request for alternative means of data subject notification is that there are only seven identified data subjects, and the 100,000 (one hundred thousand) are yet to be determined "if there are [sensitive personal information]

---

[1] *In re: Philippine National Police, NPC BN 23-110*, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (26 April 2023).
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *In re: Philippine National Police, NPC BN 23-110*, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (26 April 2023).

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

that has been viewed, accessed or downloaded."[6] PNP also stated that its investigation team is still in the process of gathering other pieces of evidence that would indicate if there are unauthorized activities.[7]

PNP also claimed that its system is already down and under maintenance and that it would conduct a Vulnerability Assessment and Penetration Testing (VAPT).[8] Lastly, the data involved in the incident are government-issued ID's and eligibilities of individuals applying to be members of the PNP.[9]

On 02 May 2023, the Commission issued a Minute Resolution with the following dispositive portion:

> Pursuant to Section 17(D) of NPC Circular No. 16-03 (Personal Data Breach Management), the Commission may require additional information, if necessary, for the proper resolution of the request for extension of thirty (30) days to submit its full report and use of alternative means to notify its affected data subjects.
>
> **WHEREFORE,** premises considered, the Commission hereby **ORDERS** Philippine National Police to **SUBMIT** within five (5) days upon receipt of this Minute Resolution proof to substantiate the request for extension of thirty (30) days to submit its full report and use of alternative means of notification to notify its affected data subjects.
>
> Should Philippine National Police fail to provide the foregoing, this case shall be submitted for resolution based on the records before the Commission.
>
> **SO ORDERED.**[10]

To date, PNP has not yet complied with the Commission's directive in the Minute Resolution. Thus, PNP failed to substantiate its request for alternative means of data subject notification and request for extension of time to submit its full report.

---

[6] *Id.*
[7] *Id.*
[8] *Id.*
[9] *In re: Philippine National Police, NPC BN 23-110*, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (26 April 2023).
[10] *In re: Philippine National Police, NPC BN 23-110*, Minute Resolution dated 02 May 2023, at p. 1.

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

In the best interest of the affected data subjects and to allow them to take the initial and necessary safeguards to protect their personal data against the possible implications of the breach, the Commission deems it proper to grant PNP's request for alternative means of data subject notification. However, the Commission emphasizes that individual data subject notification is still necessary.

The Commission allows alternative means of notification in this incident in order to serve the intended purpose of data subject notification. While individual notification is still necessary, alternative data subject notification will inform the affected data subjects of the breach incident affecting their personal data.

Moreover, the Commission deems it proper to allow alternative means of notification considering that more or less one hundred thousand (100,000) are still being determined by the PNP. In line with this, waiting for further information and identification of the affected data subjects for the purpose of individual notification will most likely just delay the notification requirement. Consequently, this will defeat the purpose of data subject notification as prescribed in the NPC Circular No. 16-03, Section 18. In the meantime, alternative means of notification will allow affected data subjects to be informed of the incident and to take the necessary precautions.

Thus, the Commission grants the request for alternative means of notification in addition and not in lieu of the individual data subjects' notification.

Section 18 (C) and (D), of NPC Circular No. 16-03 provide for the content of notification and methods of alternative means of notifying the affected data subjects:

> **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:
>
> C. Content of Notification. The notification shall include, but not be limited to:
> 1. nature of the breach;
> 2. personal data possibly involved;

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

> 3. measures taken to address the breach;
> 4. measures taken to reduce the harm or negative consequences of the breach;
> 5. representative of the personal information controller, including his or her contact details, from whom the data subject can obtain additional information regarding the breach;
> 6. and any assistance to be provided to the affected data subjects.
>
> Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.
>
> 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 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)[11]

In view of the foregoing, the Commission grants PNP's request for alternative means of notification through public communication or any similar means in which the affected data subjects should be informed of the breach incident involving their personal data. The content of the notification should comply with the above-stated provision.

Further, the Commission finds that the PNP's breach incident falls under the mandatory breach notification requirement and individual data subject notification is necessary to protect them from the risk of serious harm. Section 11 of the NPC Circular No. 16-03 (Personal Data

---

[11] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §18 (C) (D) (15 December 2016) (NPC Circular 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

Breach Management) provides for conditions on when notification is required, thus:

> **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:
>
> 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**. (emphasis supplied)[12]

In this breach incident, all the elements of mandatory notification are present.

First, there are government-issued IDs and eligibilities of the PNP employees which clearly contain sensitive personal information (SPI). Further, Section 3 (l) of the Republic Act 10173 also known as the Data Privacy Act of 2012 provides for the definition of Sensitive Personal Information, thus:

> SEC. 3. *Definition of Terms.* – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:
>
> (l) Sensitive personal information refers to personal information:

[12] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §11(C) (D) (15 December 2016) (NPC Circular 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

> (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
> (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
> (3) **Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and**
> (4) Specifically established by an executive order or an act of Congress to be kept classified.[13]

Hence, it is clear that the data in the government-issued IDs and information on the eligibilities of the affected data subjects contain sensitive personal information. Thus, the first element of mandatory notification is present.

Second, there are sample screenshots provided by the Commission containing personal information that are confirmed to be documents stored in the PNP storage server.[14] This confirmation that the sample screenshots matched with the documents stored in the PNP's storage system would indubitably state that there is reason to believe that such pieces of information were accessed or acquired by an unauthorized person.

Lastly, considering that there is a certainty that an unauthorized person had access to or acquired the sensitive personal information of the affected data subjects, it cannot be set aside that this incident would not cause serious harm to the affected data subjects. Thus, the third element of mandatory notification is present.

Moreover, Section 13 of NPC Circular No. 16-03 also determines when there is a need to notify:

---

[13] An Act Protecting Individual Personal Information in Information and Communications Systemsin the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, chapter I, § 3 (l) (2012).
[14] *In re: Philippine National Police, NPC BN 23-110*, Preliminary Breach Notification Form, Data Breach Notification Management System (DBNMS) (26 April 2023).

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

> 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:
> **A. Information that would likely affect national security, public safety, public order, or public health;**
> **B. At least one hundred (100) individuals;**
> C. Information required by applicable laws or rules to be confidential; or
> D. Personal data of vulnerable groups. (Emphasis supplied)[15]

In PNP's initial breach notification, it stated in its justification for alternative means of notification that "more or less one hundred thousand (100,000) more is still to be determine if there are SPI that has been viewed, accessed or downloaded." Thus, this clearly falls under the above-stated provision wherein in this case there are more than one hundred (100) individuals affected by the breach.

Moreover, it is imperative to acknowledge that the data involved in this breach incident pertains to our nation's law enforcement personnel. This emphasizes the gravity of the situation, as any compromise affecting sensitive personal information related to our law enforcement has the potential and possible impact that would likely negatively affect national security, public safety, and overall public order.

Therefore, considering that all the elements of mandatory notification as provided in Section 11 of NPC Circular No. 16-03 and supplemented by Section 13 of the same circular on the guidelines in determining when there is a need to notify, the Commission deems it proper that individual data subject notification is necessary.

The Commission, time and again, stresses the importance of notifying the affected data subjects. The purpose of such notification is to provide the affected data subjects with the precautions and necessary

---

[15] National Privacy Commission, Personal Data Breach Management, NPC Circular 16-03, rule V, §13 (15 December 2016) (NPC Circular 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

measures to safeguard themselves against any potential repercussions stemming from the breach.

Furthermore, the Commission reiterates that its granting of the request for alternative means of notifying the affected data subjects is to complement, rather than substitute individual data subject notification. Thus, alternative means of data subject notification alone would not suffice for the notification requirement in this breach incident without complying with the individual data subject notification.

WHEREFORE, premises considered, this Commission **GRANTS** Philippines National Police's request for alternative means of notification to the affected data subjects, in addition, and not in lieu of individual data subject notification.

Further, the Commission **DENIES** the Philippine National Police's request for extension of time to submit a full report.

The Philippine National Police is hereby **ORDERED** to **NOTIFY** the affected data subjects through alternative means of notification **in addition to the individual data subject notification** and to **SUBMIT** proof of data subject notification directly to the Compliance and Monitoring Division (CMD).

Further, the Commission **DIRECTS** the CMD to issue the appropriate orders necessary to evaluate and monitor the completeness of the Philippine National Police's data breach notification and assess its breach management pursuant to NPC Circular 16-03 (Personal Data Breach Management).

SO ORDERED.

City of Pasay, Philippines.
16 August 2023.

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

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:

LC
Data Protection Officer
PHILIPPINE NATIONAL POLICE

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