IN RE: POLYTECHNIC UNIVERSITY OF THE PHILIPPINES **NPC BN 18-222**

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

RESOLUTION

AGUIRRE, *D.P.C.*;

Before the Commission is the Compliance dated 19 January 2023 submitted by Polytechnic University of the Philippines (PUP) following the Commission's directives to individually notify its affected data subjects and submit proof of notification.[1]

Facts

To recall, on 22 November 2018, PUP sent a letter to the National Privacy Commission (NPC) formally notifying the latter of an incident concerning possible information security breach.[2]

PUP alleged that on 20 November 2018, it came across a post on ZeroSecurity PH's Facebook page.[3] The post claimed that it was able to obtain three thousand eight hundred nine (3,809) email addresses from the PUP Website.[4]

On 20 May 2022, the NPC, through its Complaints and Investigation Division (CID), issued an Order requiring PUP to submit a Post-Breach Report detailing the incident that prompted the notification of the

[1] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[2] Notification Letter to the Commission, 22 November 2018, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2018).
[3] *Id.*
[4] *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

incident.[5] In compliance, PUP submitted its Post-Breach Report on 07 June 2022.[6]

In its Post-Breach Report, PUP reported that it cross-referenced all three thousand eight hundred nine (3,809) emails with its PUP Student Information System (SIS).[7] It determined, however, that only nine hundred ninety-one (991) email addresses matched with the SIS.[8] PUP confirmed that all the nine hundred ninety-one (991) matched email addresses "belong to student[s] who have already graduated or have dropped out from the University."[9]

PUP also claimed that the investigation on system logs revealed that "there was no direct access to the system database and that the records were compiled from different sources and not from the [SIS]".[10] PUP explained that "no hacking was done but mere exploitation of an old list (physical copy) of email addresses of students and some faculty members."[11]

Further, PUP maintained that it notified all the affected data subjects through a prompt in the SIS to change their passwords and "take other important measures to ensure that their account is secured."[12]

On 10 November 2022, the Commission issued an Order where it held PUP's notification "inadequate because it lack[ed] the contents required in an appropriate notification to the affected data subjects."[13] Thus, the Commission directed PUP to individually notify its affected data subjects:

> **WHEREFORE**, premises considered, Polytechnic University of the Philippines is hereby **ORDERED** to comply with the following **within fifteen (15) days** from the receipt of this Order:

---

[5] Order, 20 May 2022, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[6] Post-Breach Report, 07 June 2022, at 1, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[7] *Id.* at 2.
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] Post-Breach Report, 07 June 2022, at 3, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[13] Order, 10 November 2022, at 5, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).

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. **NOTIFY** its affected data subjects and **SUBMIT** proof that it individually and directly informed its affected data subjects; and
2. **SUBMIT** proof of the security measures it implemented.

SO ORDERED.[14]

In compliance with the Order, on 19 January 2023, PUP submitted a list of the names of the nine hundred ninety-one (991) affected data subjects with their corresponding email addresses.[15] It also submitted the generated email delivery receipts which showed a copy of the notification sent, its date of sending, and the recipient email addresses.[16]

PUP also enumerated the information security solutions it implemented and attached screenshots of the dashboard of each security solution.[17] These include:

1. Next Generation Firewall Using Checkpoint – this can detect and block sophisticated attacks by enforcing security policies at the application, ports, and protocol levels;[18]
2. Vulnerability Assessment Tools Using Teneble.IO Solution – this is a tool designed to automatically scan for new and existing threats that can target an application;[19]
3. Network Monitoring & Performance Management Tools Using Solarwinds Solutions – these tools gather and analyze network data to provide network administrators with information related to the status of network appliances, network traffic or the sources of network problems and traffic anomalies;[20]
4. Network Access Control Using Forescout Solutions – this enables PUP to restrict unauthorized or non-compliant devices and users from accessing the corporate network and helps

[14] Order, 10 November 2022, at 6, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[15] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *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

ensure that all devices connected to PUP network are compliant with its security policies; and[21]

5. Patch Management Tools using ZENWorks Solutions – this gives the administrator control over operating system, platform, or application updates. This is often necessary to correct errors, bugs, or vulnerabilities in the software.[22]

Issue

Whether PUP notified its data subjects and sufficiently addressed the breach and implemented measures to prevent its recurrence.

Discussion

The Commission resolves to close the matter. PUP individually notified its affected data subjects, submitted sufficient proof of notification, and implemented security measures to prevent the recurrence of the breach. PUP sufficiently complied with the Commission's Order dated 10 November 2022.

It is the obligation of a Personal Information Controller (PIC), such as PUP, to ensure that it promptly notifies its affected data subjects of the breach.[23] Section 18 (D) of NPC Circular 16-03 (Personal Data Breach Management) 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:
>
> . . .
>
> 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.[24]

---

[21] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[22] *Id*.
[23] National Privacy Commission, Personal Data Breach Management, Circular No. 03, Series of 2016 [NPC Circ. No. 16-03], § 18 (A) (15 December 2016).
[24] *Id*. § 18 (D). Emphasis supplied.

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 18 (C) of the NPC Circular 16-03 also provides the information required to be provided to 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;
> 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; and
> 6. any assistance to be provided to the affected data subjects.[25]

In this case, PUP individually notified its affected data subjects of the breach through electronic mail.[26]

In compliance with the directive to submit proof that it individually notified its affected data subjects, PUP submitted screenshots of the electronic mails it sent to the individual email addresses of nine hundred ninety-one (991) affected data subjects.[27] Due to the large number of the recipients, PUP sent the notification in four (4) batches.[28] The first, second, and third batches each resulted in the notification of two hundred and fifty (250) affected data subjects, while the fourth batch resulted in the notification of two hundred and forty-one (241) affected data subjects.[29]

---

[25] *Id*. § 18 (C).
[26] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[27] *Id.*
[28] *Id*.
[29] *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

PUP also submitted to the Commission a copy of the individual notification it sent to the affected data subjects.[30]

The notification sent by PUP sufficiently informs the affected data subjects of the nature of the breach and the personal data possibly involved in the breach:

> The 991 email addresses that matched with the email addresses published by the 'hackers' are old records. The email addresses belong to students who already graduated or have dropped out from the University. Further investigation conducted by ICTO on system logs reveals that there was no direct access to the system database and that the records were compiled from different source/s and not from the Students Information System as claimed by the 'hackers. Technically, no hacking was done but mere exploitation of an old list (physical copy) of email addresses of students and some faculty members.[31]

Further, the notification enumerated the measures PUP took to address the breach and to reduce the harm or negative consequences of the breach.[32] It enumerated PUP's actions, such as cross-checking the email addresses listed in the Facebook post with the SIS database; placing prompt in its SIS informing students to change passwords and secure account; conducted an audit of the System Log; checking the SIS' vulnerabilities; and securing and improving the security measures in the program.[33] It also contained the contact information of PUP's Data Protection Officer in case the affected data subjects should require further assistance.[34]

As part of a PIC's data breach management, it should implement policies and procedures for managing security incidents, including data breaches, following Section 4 of NPC Circular 16-03.[35] This includes ensuring implementation of organizational, physical, and technical security measures and data privacy policies intended to prevent or minimize the occurrence of a data breach and assure the timely discovery of a security incident:

---

[30] *Id*.
[31] *Id*.
[32] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[33] *Id.*
[34] *Id*.
[35] NPC Circ. No. 16-03, § 4.

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 4. *Security Incident Management Policy*. A personal information controller or personal information processor shall implement policies and procedures for the purpose of managing security incidents, including personal data breach. These policies and procedures must ensure:
>
> . . .
>
> B. Implementation of organizational, physical and technical security measures and personal data privacy policies intended to prevent or minimize the occurrence of a personal data breach and assure the timely discovery of a security incident[.][36]

PUP demonstrated that it implemented security measures to prevent or minimize the occurrence of a data breach. As verified by the CID of the National Privacy Commission:

> PUP redeveloped its web security and improved technical security measures particularly the Student Information System.
>
> . . .
>
> The security measures implemented after the incident enabled PUP to strengthen its organizational and technical measures to protect the personal data against any accidental or unlawful destruction, alteration, and disclosure.[37]

In addition, PUP submitted further proof of the information security solutions and measures that it implemented.[38] It explained the various software it installed for the security of its systems in relation to the incident that transpired on 20 November 2018.[39] PUP presented screenshots of the dashboards showing that each software is active and running in its systems.[40] Given PUP's submissions, the Commission finds that the measures undertaken by PUP have sufficiently addressed the breach and prevent a recurrence of the incident.

---

[36] *Id*. § 4 (B).
[37] Final Breach Notification Evaluation Report, 14 October 2022, at 8, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2022).
[38] Compliance of PUP to Order dated 10 November 2022, 19 January 2023, Annex, *in* In re: Polytechnic University of the Philippines, NPC BN 18-222 (NPC 2023).
[39] *Id*.
[40] *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

WHEREFORE, premises considered, the Commission resolves that the matter of NPC BN 18-222 In re: Polytechnic University of the Philippines is **CLOSED**.

SO ORDERED.

City of Pasay, Philippines.
03 February 2023.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

WE CONCUR:

Sgd.
JOHN HENRY D. NAGA
Privacy Commissioner

Sgd.
NERISSA N. DE JESUS
Deputy Privacy Commissioner

Copy furnished:

MANUEL M. MUHI
President
Polytechnic University of the Philippines

COMPLAINTS AND INVESTIGATION 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

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