Form 4
UNIVERSITY OF THE PHILIPPINES
Mandatory Personal Data Breach Notification for Data Subjects[1]

University of the Philippines (insert if System or CU)
Address
Contact information

Insert date

Subject: Data Breach dated (insert date) of (insert data processing system or data base)

Dear (insert name of data subject)

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: (insert data involved in the data breach)

Nature of the breach

Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject

Describe the likely consequences of the personal data breach.

Measures taken to Address the Breach

Provide information on measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.

Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.

Describe steps the organization has taken prevent a recurrence of the incident

Measures taken to reduce the harm or negative consequences of the breach.

Describe actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident. Assistance to be provided to the affected data subjects. Include information on any assistance to be given to affected individuals.

Do not hesitate to contact our Data Protection Officer for further information:

1

We undertake to provide more information to you as soon as they become available.

Sincerely,

SOURCE: NPC Advisory 2018-02

Please be guided by the following provision in the UP Data Privacy Manual:

SECTION 31**.** The concerned office shall notify or cause the UP ITDC or CU IT office, or other relevant office, to send notice to the data subjects affected by a personal data breach, subject to the following procedures:

31.1. When Should Notification Be Done. The data subjects shall be notified **within seventy-two (72) hours upon knowledge of, or reasonable belief by, UP or its 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 supplemented with additional information at a later stage on the basis of further investigation.

31.2. Exemption or Postponement of Notification. If it is not reasonably possible to notify the data subjects within the prescribed period, UP shall request the NPC for an exemption from the notification requirement, or the postponement of the notification. UP may be exempted from the notification requirement where the NPC determines that such notification would not be in the public interest or in the interest of the affected data subjects. The NPC 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 NPC Circular 16-03, and other risks posed by the personal data breach.

31.3. Content of Notification. The notification (Form 4) 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 UP, 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.

Where it is not possible to provide the foregoing information all at the same time, they may be provided in phases without undue delay.

31.4. Form. Notification of affected data subjects shall be done individually, using secure means of communication, whether written or electronic. The University 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. UP 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, UP may seek the approval of the NPC 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 University shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the breach.