Form 3
University of the Philippines
Mandatory Personal Data Breach Notification for the National Privacy Commission[1]

General cause (Indicate if due to malicious attack, system glitch, human error or a combination of the same)

Specific cause

Indicate if the notice includes a request to the NPC ie Request for postponement of notification to NPC and/or data subjects, Request for alternative means of informing data subjects See NPC 2016-03

Describe how the breach occurred and the data processing system vulnerability that allowed such breach

Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.

[1] Email the accomplished form to the UP System (dpo@up.edu.ph) as well as the proper DPO (PGH, PGC, CU etc) so that the DPO will be able to report to the NPC pursuant to the provisions of the UP Data Privacy Manual SECTION 30**.** The concerned office shall notify the NPC of a personal data breach subject to the following procedures:

30.1. When Notification Should Be Done. The NPC shall be notified by the proper DPO through the NPCs data breach portal https://dbnms.privacy.gov.ph/login within seventy-two (72) hours upon knowledge of or the reasonable belief by UP or its personal information processor that a personal data breach has occurred.

30.2. Delay in Notification. Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. UP need not be absolutely certain of the scope of the breach prior to notification. Its inability to immediately secure or restore integrity to the information and communications system shall not be a ground for any delay in notification, if such delay would be prejudicial to the rights of the data subjects. Delay in notification shall not be excused if it is used to perpetuate fraud or to conceal the personal data breach.

30.3.When Delay is Prohibited. There shall be no delay in the notification if the breach involves at least one hundred (100) data subjects, or the disclosure of sensitive personal information will harm or adversely affect the data subject. In both instances, the NPC shall be notified within the 72-hour period based on available information. The full report of the personal data breach must be submitted within five (5) days, unless UP is granted additional time by the NPC to comply.

Approximate number of data subjects or records involved. Does it involve at least 100 data subjects? (Note no postponement of notification is allowed in this case) Provide details to explain the answer.

Provide a description of how the breach will affect UP and the data subjects involved

Indicate the name of the Data Protection Officer or responsible person reporting the breach

Indicate all the sensitive personal information involved[2]

Indicate all other information involved that may be used to perpetrate fraud[3]

Specific measures to address the breach including the results of the investigation conducted.

Actual measures to secure or recover the personal data involved

Actual measures taken to mitigate harm

The actual manner used to notify data subjects and including any assistance extended to them

---

[2] *Sensitive personal information* refers to personal information:

> **(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.

[3] 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; email addresses; biometric data; copies of identification documents, licenses or unique identifiers like PhilHealth, SSS, GSIS, TIN numbers; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.

Actual or proposed orientation materials addressing the vulnerability identified

Record type involved (e.g digital or physical, email, email with attachments)

Data subjects involved (Own employees, vulnerable groups e.g. students, research participants[4], customers, etc)

[4] These include minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a personal information controller or personal information processor require special protection. NPC Advisory Opinion 2018-077 and NPC Advisory Opinion 2021-043.