University of the Philippines Diliman
Data Protection Team

upd.edu.ph/privacy
dpo.updiliman@up.edu.ph
(632) 981-8500 local 2621

23 March 2019

ADVISORY OPINION

Reference No. DPO 19-12

FOR : **[Redacted]**
[Redacted]

SUBJECT : **Request to Review NDA**

Dear [Redacted]:

We respond to your request for advice on the Non-Disclosure and Confidentiality Agreement (NDA) which you patterned from the version of the [Redacted]**.** We commend your draft as it faithfully adopts all key points in the [Redacted] NDA.

We have humbly observed that while [Redacted] NDA is good, it may have overlooked a number of items related to data protection. Understandably, your own version (adopted from [Redacted] NDA) also acquired these possible shortcomings. We note the following respectful observations on [Redacted] NDA:

Sections 1-4

[Redacted] NDA defines privileged information, confidential information and sensitive personal information. We respectfully note that [Redacted] NDA may have overlooked to define the most fundamental type of information protected by the Data Privacy Act: *personal information*.

Section 6

[Redacted] NDA requires our faculty and staff that they themselves implement "organizational, physical and technical security measures." Under Section 25 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 ("DPA IRR"), this is the responsibility of the organization, not its people. Our faculty and staff may raise concerns why we are shifting these obligations to them. What we can do is impose specific *operational measures* to our people – and perhaps minimize imposing to our people responsibilities which should be the responsibility of the institution.

Requirements of strict confidentiality and processing

While [Redacted] NDA is admirable in that it prevents disclosure of "confidential/privileged information" in *"personal dealings"*, it may have overlooked to lay out the following regulatory requirements:

- Operate and hold *personal information* as well as *sensitive personal information* under **strict confidence** (DPA IRR Sec. 26 (d) par. 2)
- Process personal data only if there is a legitimate purpose (DPA IRR Sec. 18 (b))
- Ensure the processing of personal data is necessary and not excessive to its purpose (DPA IRR Sec. 18 (c))
- No employee of the government shall access sensitive personal information unless there is a security clearance (DPA IRR Sec. 31(a)(1))

Acceptable Use Policy, Restricted Access and Security Clearances

NPC Circular 16-01 requires government employees to comply with the Acceptable Use Policy, restricted access and security clearances imposed by their organization. It may be advisable that [Redacted] NDA includes a statement regarding these.

Specific operational measures

In addition to [Redacted] NDA's requirement of preventing "confidential/privileged information" to be used in *"personal dealings"*, it may be advantageous to also impose *specific operational* measures to our people. The obligations of a personal information processor in DPA IRR Sec. 44(b) may be used as framework.

Since you patterned your own NDA from [Redacted] NDA, it is natural that your version acquired the above possible oversights. To address these, for your consideration, we drafted the attached **"[Redacted]"**. This [Redacted] may be executed as an attachment to your NDA without revising your own NDA's contents. The legal bases of the provisions in the [Redacted] are stated inside comment boxes.

Please feel free to reach out for additional concerns.

Yours,

Elson Manahan
Data Protection Officer
University of the Philippines Diliman