University of the Philippines Diliman
DATA PROTECTION TEAM

MEMORANDUM

26 October 2018

Reference No. DPT 18-22

FOR : [redacted]

THRU : [redacted]

SUBJECT : **Non-Disclosure and Confidentiality Agreement from OC Memorandum No. 18-190**

Dear [redacted]:

We thank the [redacted] in your attention to data privacy by conducting a meeting on the Non-Disclosure and Confidentiality Agreement ("NDA") provided by the Office of the Chancellor through OC Memorandum No. 18-190. As the NDA did not come from our Data Protection Team, we herein respectfully provide our humble comments to the NDA.

Data Protection

In addition to the lack of a statement on breach, we have humbly observed that the NDA may have overlooked the following aspects of data protection:

Sections 1-4

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

Section 6

The 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 the 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 the NDA includes a statement regarding these.

Specific operational measures

In addition to the 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.

Breach of contract

There may also be s a need to include a statement that deals with a faculty or employee's breach of the NDA. Without a statement on breach, the NDA's effectiveness is considerably limited.

Along with this Memorandum is a suggested **"Annex for Breach and Data Protection"** which your good College may optionally use to address our respectful comments above. This Annex may be executed as an attachment to the NDA without modifying the contents of the NDA.

The legal bases of the provisions in the Annex are indicated as comment boxes in the right margin of the Annex.

Please feel free to reach out for clarifications or further concerns.

Yours truly,

(Sgd.) Elson B. Manahan
Data Protection Officer
University of the Philippines Diliman