University of the Philippines Diliman
Data Protection Team

upd.edu.ph/privacy

dpo.updiliman@up.edu.ph

(632) 8255 3561

17 October 2019

ADVISORY OPINION

Reference No. DPO 19-47A

FOR : [redacted]

SUBJECT : **Clarifications Regarding Data Privacy Act**

Dear [redacted]:

We applaud your initiative to conduct again another data privacy seminar. We apologize for our delay in providing the following responses:

Inquiries	UPD DPO Opinions
1. Definition of "Official Message" In the memo, "Clarification on Privacy and Confidentiality Notice…," it was indicated that being an "official message" from UP is one of three conditions that together will require the use of the privacy notice. We'd like to ask for examples of "an official UP message is."	An official UP Message is one that is either a message (1) made in the performance of a role or function of a UP staff, faculty REPS, researcher or personnel; (2) a message for or on behalf of a UP or a unit or office of UP; or (3) wherein it will be UP, and not the sender in his/her personal capacity, will be liable.
2. Use of Privacy and Confidentiality Notice Similar to the above, given the nature of an official message, who are the ones authorized/required to use the notice? Does it apply only to heads of units/department chairs or just university administration officials? Is this still the prescribed format, (we could, I know, adapt it depending on context).	UP faculty, visiting faculty, staff, Research, Extension and Professional Staff (REPS), researchers, UP contractual personnel and Non-UP contractual personnel who are sending an official message as defined above must include the Privacy and Confidentiality Notice.
3. Disclosure within and across UP Units To what extent can an employee know who an applicant is for a particular position? On	This is a valid and important question. From a *"disclosure"* point of view, there is no disclosure to an external party if we transfer

the grounds that since everyone will work with whoever is chosen, do they have some legitimate interest in the hiring process? To what extent? This inquiry also raises some general issues. Although we are told that UP is a single juridical unit (no breach when information is shared within UP), we are also advised to disclose information on a need-to-know basis, and prevent access to our documents apart from those involved in our work and one's superiors. Given these two seemingly conflicting notions, to what extent does the DPA cover disclosures within and across UP units? If it can be shared within/across UP units, is there a restriction as to whom? Which information remains private, and which ones are not and thus can be shared/discussed, etc. within/among/between UP units?	information within UP units. From an *"authorized processing"* point of view, only those who have a need-to-know are authorized to receive and process information. We are thankful that you raised this matter and we acknowledge the need to clarify this matter to the UP Diliman community.
4. Posting of Photos on Social Media Photos can be posted on social media on the grounds of "public interest," as well as journalistic, literary, and research purposes. Does this mean we have to ask for the consent of individuals before we can post photos of, say, events at the [redacted] website, or can we just post them straightaway since our site is of public interest (part of information literacy)? Following the principle of transparency, is it enough to tell people that we will be taking photos and that we will be uploading it to the [redacted]'s Facebook page, the website (e.g., as part of the site dedicated to lectures), or use them for [redacted]'s promotional activities? Does posting on the website and social media both cover "public interest" or journalistic purposes? Also, how do the photo posting-privacy guidelines impact individual staff/faculty? If a staff posts a photo of students on his personal social media account, does that qualify as public interest or journalistic purpose?	We commend your grasp of the nuances of the scope of applicability to data privacy. The Data Privacy Act of 2012 and its Implementing Rules and Regulations do not include "public interest" *per se* as a ground to process information. Posting in social media is not classified as "journalistic purposes" because this covers the practice of journalism on an industry level, a professional level or a campus journalism level. Pictures wherein the intended subject matter of the image are individuals cannot be posted on social media. Wide shot and panoramic pictures can be posted in social media as long as the intended subject matter of the image is the event. Hence, if the picture is an image of the event in general and no individuals are predominantly featured, it can be posted. This is admittedly difficult to implement and subjective and hence even foreign jurisdictions have varying rules. This boils down to case-to-case determinations whether pictures may be posted or not.
5. The Use of BCC A similar inquiry is whether and to what extent the use of bcc among members of a UP unit is necessary.	The use of BCC and forwarding of emails share a common concern: there may be situations wherein a person is unaware that his/her email message (and hence identity) is being shared to another. Generally, sharing the identity of a person through BCC or forwarding is prohibited. However, it may

	be permitted when the person who receives the BCC or the forwarded message has a right to be aware of the conversation. Examples include: a work superior having the right to know the a work-related matter being discussed; the role or function of a person grants the person the right to know the conversation; or a matter is being reported or consulted to the proper authority. BCCs may be used in announcements wherein the recipients do not need to know each other. For example, for an email reminding habitually late staff of their delinquency, an email may be sent to all of them in BCC.
6. Definition of Personal Information The DPA's definition of personal information is broad, and an exemption refers to "information about any individual who is or was an officer of a government institution that relates to the position or functions of the individual under Section 4(a)." Does this cover everything that an employee does: activities, documents, whereabouts, other actions that are all performed as UP employees? If so, how do we balance the privacy of UP employees as individuals and private citizens, and as public servants/government employees whose tasks affect his/her colleagues who arguably have a legitimate interest in what he/she does? Are some of her tasks/documents private, while others are not? Which are office matters, and which ones are private?	Only the following information about a government employee is exempt from the prohibitions of the Data Privacy Act of 2012: (1) The fact that the individual is or was an officer or employee of the government institution; (2) The title, business address and office telephone number of the individual; (3) The classification, salary range and responsibilities of the position held by the individual; and (4) The name of the individual on a document prepared by the individual in the course of employment with the government. Other information about government employees are still protected by the law.
7. Mailing List and Data-Processing System The mailing list of the [redacted] covers around 5,900 individuals, their names and email addresses. Does this mean we have to register our data processing system to the National Privacy Commission, or does the NPC advisory on the log book pertain only to the keeping of sensitive personal information of at least 1000 individuals? Does this also apply to our deadline mailing lists, which now exceed 1,000 email addresses? There are no sensitive personal information there, however. Here are our other lists: · Online registration for all our events/lectures	The mailing list is not a "data processing system" itself. The data processing system there is the email service. The UP Diliman Data Protection Officer has already registered with the National Privacy Commission UP Mail and UP Diliman Webmail as data processing systems of UP Diliman.""

· Deadline for graduate program application · Job opportunities · Inquiry forms for Rentals Please advise us of further data-protection measures (registration with the NPC, etc.).	
8. Question on Transparency Regarding Storage As part of the principle of transparency, do we have to tell people exactly what software we use in storing electronic information? ([redacted]) Or will a generic phrase, "cloud services" suffice? Also, am I correct to say that the names of the personal information processor must be indicated?	Cloud services" and "cloud storage locations" will suffice. There is no need to specify what specific software product is used. The names of personal information processors may not be disclosed since they are only agents acting as subcontractors of UP Diliman. Since UP Diliman merley outsources its functions to these personal information processors, they are only acting under the control of UP Diliman and the liability is still with UP Diliman.
9. Clarification on Requirements and Procedures for Disclosure Having read the advisory opinions of the NPC and the DPO, may we ask for general procedures for releasing information? Much of what I know is that we have to establish the transparency (purpose) and legitimacy of the request and redact any personal information, and whether consent is required, etc. But once established that such particularly information can be released, can we then proceed to release the information accordingly? Must the release of the data be approved in writing by the chancellor or by the dean, or will the (written?) authorization of the heads of office (e.g., College Secretary for student-related information) suffice? I cannot seem to find a page from the DPO or the NPC listing down procedures for the release of information? Your guidance will help us draft the Privacy Manual of the Asian Center, and can help us disseminate the information to our colleagues.	The reason why the NPC and the UP Diliman DPO has no procedures for the release of information is that each process in an organization is unique and has very specific requirements. For example, the procedure in releasing grades of an alumni is very different from the procedure of releasing the SALN of an employee. No new procedures should be created, the Privacy Focal Person only has to review existing procedures and processes and suggest improvements to protect data. In lieu of specific procedures, the following guiding principles should be followed: (1) Follow the privacy principles of transparency, legitimate purpose, and proportionality; (2) Institute organizational, physical, and technical security measures; (3) Comply with the UP Diliman Privacy Policy; (4) Comply with the UP Diliman Data Subject Rights and Responsibilities; (5) Comply with the UP Diliman Data Protection Guidelines for Work Processes; (6) Obtain and record consent when necessary; and (7) In case of doubt, the concerned staff or faculty should consult the Privacy Focal

	Person or Data Protection Officer. Privacy Focal Persons should be guided by the UP Diliman Privacy Management Program Framework. The UP Diliman Data Protection Team will promulgate the following policies in coming months: (1) Privacy Manual; (2) Information Security Policy; (3) Records Management Policy; and (4) Organizational and Physical Security Measures Policy.
10. Data Breach Procedure Does UP already have a template for reporting data breaches? I am just familiar with the information from the NPC page.	There is no form that should be accomplished for reporting but the matters that should be reported and the manner of reporting are in the UP Diliman Security Incident Management Policy.
11. Log Book An NPC Advisory notes that log books contain personal if not sensitive information, does this mean that log books must not display the names, times of arrival, etc., of all previous visitors for all future visitors to see? Should a log in system be designed or implemented in such a way as to individualize log-ins, say, through an electronic form or at least slips of paper?	Yes, ideally log books should be designed to individualize log-ins to prevent visitors from viewing information of other visitors. It is a welcome innovation if the [redacted] will implement this type of privacy security measure. However, the UP Diliman Data Protection Team recognizes the logistical and technical difficulties of requiring this from all UP Diliman units and offices. Hence, utilizing the purpose, necessity and balancing tests in NPC Advisory Opinion Nos. 2018-061 and 2018-020, UP Diliman has not yet imposed any requirement on logbooks.

Please feel free to forward the above responses to all concerned UP Diliman staff and faculty. Again, we express our appreciation to your vigilance to your attention to detail in various privacy concerns.

Regards,

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