PRIVACY NOTICE FOR UNIVERSITY OF THE PHILIPPINES PERSONNEL

I. INTRODUCTION

The University of the Philippines is committed to complying with the Data Privacy Act of 2012 (DPA) http://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/ in order to protect the right to data privacy of UP personnel (the data subject).

This notice explains in general terms the purposes, and legal bases, for the processing of the typical examples of personal and sensitive personal information that UP collects from its personnel, the measures in place to protect data privacy, and the right to access and correct the same. Please note that this document does not contain an exhaustive list of all of UP's processing systems, as well as the purposes and legal bases for processing. UP websites, as well as other UP offices or units, may provide other privacy notices pertaining to specific processing systems.

Under the DPA, personal information may be processed (e.g., collected, used, stored, disclosed): (1)with the consent of the data subject; (2) pursuant to a contract with the data subject; (3)when it is necessary in order for UP to comply with a legal obligation; (4) to protect vitally important interests including life and health; (5) in order to respond to a national emergency; (6) to comply with the requirements of public order and safety; (7) to fulfill the functions of public authority; or (8) pursuant to the legitimate interests of UP or a third party, except where such interests are overridden by the data subject's fundamental rights.

Sensitive personal information (e.g., confidential educational records, age, birthdate, civil status, health, religious affiliation) on the other hand may be processed: (1) with the consent of the data subject; (2) when such is allowed by laws and regulations, and such regulatory enactments provide for the protection of such information, and the consent of the data subject is not required. Processing may also be done when needed to protect the life and health of the data subject, or another person, and the data subject is unable to legally or physically express consent, in the case of medical treatment; or needed for the protection of lawful rights and interests of natural or legal persons in court proceedings, and for the establishment, exercise or defense of legal claims, or where provided to government or public authority.

Section 4 of the DPA also provides that among others such Act does not apply to the following:

(a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(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;

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic, literary or research purposes;

(e) Information necessary in order to carry out the functions of public authority.

In most cases UP processes your personal data in order to carry out its functions as the National University pursuant to the UP Charter and its right to academic freedom under the 1987 Constitution, comply with legal obligations, lawful issuances or orders of other public authorities, as well as contractual obligations to you, and to pursue its legitimate interests.

Personal data refers to personal and sensitive personal information as defined under the DPA.

The term *UP/University/us* refers to the relevant University of the Philippines System and Constituent University (CU) offices.

For the sole purpose of this notice the term *you/your/University personnel* refers to applicants for UP posts, including those covered by contract of services, past and present UP employees, as well as non-employees engaged by UP to perform personnel services pursuant to contract including, for example, lecturers, visiting professors, professors emeriti.

Please note that certain purposes for the processing of personal and sensitive personal information may apply only to certain personnel (e.g., employees or academic staff).

II. SOURCES AND CATEGORIES OF PERSONAL DATA

You provided UP with various personal data when you applied for a post. You may have attached documents, as well as references or recommendations. When you submitted your application and provided such references or recommendation letters, you granted consent, or authorized UP, to verify such information by securing relevant documents from third

parties (e.g., academic institutions), and obtained the prior consent of third parties providing you with a reference or recommendation letter for UP to process their personal information in connection with your application.

In the course of your employment or engagement with UP, you accomplish or sign forms required by law or lawful issuances of public authorities (e.g., Civil Service Commission [CSC] Personal Data Sheet, Statement of Assets and Liabilities and Net Worth [SALN], Government Service Insurance System [GSIS], PhilHealth, Home Development Mutual Fund [HDMF or Pag-IBIG]) or file applications in connection with your employment or engagement (application for renewal of appointment or tenure for academic staff, leaves, benefits and the like).

During your employment or engagement with UP, you (and in some instances in collaboration with others) produce as part of your functions documents, records, publications, research, minutes, records of proceedings and the like containing your personal data.

Some forms require you to provide a photograph. In some instances, your image is captured when UP documents, records, publishes, broadcasts, transmits, uploads or streams University activities or events.

UP operates closed circuit television (CCTV) systems for the safety and security of members of the UP community including personnel, students, alumni and guests, as well as its buildings, surrounding premises and assets. In the course of operating such CCTV systems, UP may capture your images.

In the case of some offices, biometric information may be also be used to check attendance and secure such offices.

UP may also collect publicly available information about you.

The categories of personal information that UP processes, usually through paper based or electronic means, include:

- **Personal Details**: Name, past or present addresses, provincial address, contact details, birthdate, birthplace, age, gender, civil status, religion, citizenship, signature and such other information found in Civil Service Form No. 212 – Personal Data Sheet; name of father, mother, spouse, children and other family members as required by, for example, GSIS forms or for providing benefits to dependents, SALN.
- **Educational Background:** Official Transcript of Records or True Copy of Grades, Diplomas, Educational Attainment, etc.;

- **Government-Issued Identification**: GSIS Number (Common Reference Number), taxpayer identification number (TIN), PhilHealth Number, Pag-IBIG Fund (HDMF) Number, UP employee number, etc.;
- **Health information**: height, weight, relevant medical details, etc.
- **References:** Names, contact details, employment details;
- **Information Related to your Employment or Engagement**: Service record, recruitment and performance ratings, comments, feedback, succession planning, skills and competencies, and other work-related qualifications (other relevant training, publications, research, extension work, awards and the like) security data, disciplinary records, and background check reports, your personal information contained in reports, documents or records you produce during your employment or engagement and other similar information;
- **Emergency Contacts**: Names, addresses, other contact details;
- **Photographs/Images/Biometric information** as discussed above.

III. PURPOSES FOR THE PROCESSING OF PERSONAL DATA

UP processes your personal data for the following purposes:

a. For those applying for posts:
    1) To process submitted forms and documents bearing personal information for the purpose of determining the fitness of the applicant for the position applied for;
    2) To facilitate the conduct of mandatory pre-employment examinations;
    3) To facilitate planning and staffing;
    4) To verify the applicant's identity, prevent identity fraud and conduct reference or background checks;
    5) To communicate with you regarding your application;
    6) In the event you are not selected for a post, UP may, at its sole discretion and with your consent, retain your application and supporting documents in order for UP to consider you for other posts for which you appear to be qualified.

b. For those employed or engaged by UP (note that as stated above, some purposes apply only to employees and to certain categories of employees):
    1) To enable UP to perform its mandate pursuant to Republic Act No. 9500 and exercise its right to academic freedom under the 1987 Constitution;
    2) To verify your identity and prevent identity fraud;
    3) To facilitate your employment or engagement, which includes processing your pre-appointment requirements, including medical clearance;
    4) To perform personnel actions such as the issuance or renewal of your appointment or contract, to act on your tenure application where applicable, process promotions, process your applications for leaves, retirement and the like.

5) To facilitate entry into contracts involving UP and third parties, such as with a government depositary, where UP will directly deposit compensation of employees, the UP Provident Fund and its benefits, and the like;
6) To communicate with you regarding matters related to your employment or engagement and other legitimate concerns;
7) To create/issue, modify and cancel/delete vehicle stickers or passes, clearances or access to UP's information and communications technology (ICT) based data processing systems, including email;
8) To maintain employee records or records of your contract(s), as required by law;
9) To assess your performance and competencies;
10) To provide you with available training and development opportunities beneficial to you and UP;
11) To process your applications for grants, scholarships, fellowships, travel authorities, attendance in seminars, conferences and the like as well as other similar applications in the case of qualified personnel;
12) To process your payroll, allowances, and other benefits, and make direct deposit of payments to your bank account;
13) To comply with the requirements of applicable laws and issuances of public authorities, such as the filing and remittance of taxes, payment of mandatory contributions, processing of your Statement of Assets, Liabilities and Net Worth (SALN);
14) To provide, facilitate or manage health and other welfare-related services, when available, to qualified personnel and their dependents, subject to UP's rules;
15) To comply with internal processes and legal requirements in the administration of disciplinary proceedings;
16) To investigate and resolve work-related incidents;
17) To provide a safe workplace, and secure UP premises from threats, theft, robbery, fraud, legal liability, and similar incidents;
18) To manage the assets and documents that may have been released to you in the course of your employment with UP;
19) To process the disbursement of expenses that may have been incurred by you in the performance of your functions;
20) To process any certifications, or any other documents that you may request from UP in relation to your employment or engagement;
21) To establish a contact point in the event of an emergency involving you, your colleagues, or third parties;
22) To comply with the obligations stipulated in your employment or engagement contract;
23) To conduct audits, or investigate a complaint or security threat;
24) When so required, to process the termination of your employment or engagement;

25) When so required, to settle accountabilities upon termination of your employment or engagement;
26) To compile statistics and conduct research, subject to the provisions of the DPA, and applicable research ethics guidelines, in order to carry out its mandate as the National University;
27) To enable you to participate, where applicable, in selection processes, such as for the selection of the Faculty or Staff Regent, and the like;
28) To comply with other applicable statutory and regulatory requirements, including directives, issuances by, or obligations of UP to any competent authority, regulator, enforcement agency, court, or quasi-judicial body;
29) In order to issue your UP radio frequency identification (RFID) card, UP will process your name, employee number and photograph. A unique randomly generated number, as well as your employee number, will be encoded in the RFID tag or chip of your UP ID such that these will be the only information that can be read by a compatible RFID reader.

UP, using its RFID readers, will process the abovementioned information when you tap or wave your UP ID card in close proximity to such readers to regulate access to UP buildings in order to supplement other security measures in place, and provide you with RFID enabled services in UP offices, where these are applicable or available.

UP has a legitimate interest in securing the UP community, its buildings and other assets, and adopting means in order to provide services in a more efficient manner. Rest assured that UP will process the above UP RFID information only for the abovementioned, and other compatible purposes, and for such periods allowed by the DPA and other applicable laws. UP has adopted appropriate measures to safeguard your right to data privacy over your UP RFID information.

c. To establish, exercise, or defend legal claims;
d. To fulfill other purposes directly related to the above-stated purposes; and
e. For such other purposes as allowed by the DPA and other applicable laws.

IV. DISCLOSURES

Examples when UP discloses information as allowed by the DPA or other applicable laws, or with your consent, include:

a. disclosing your name, position or function, office address, and other relevant information that are exempt from the coverage of the DPA in the relevant UP site, office rosters, or directories and the like, for public information purposes, or as required in order to comply with the requirements of issuances, such as requirements for the Transparency Seal;

b. disclosing that you are the recipient of a grant, or any other discretionary benefit of a financial nature, given by UP or the Philippine government, as allowed by Section 4 (c) of the DPA;
c. disclosures for your benefit or in support of your interests (such as those intended to enable you to participate in exchange programs, conferences, trainings, academic and other similar competitions or events), or to apply for, receive and comply with terms and conditions of scholarships, grants and other forms of assistance, or to be considered for and to receive awards with your consent;
d. disclosures in order to enable UP to participate in university ranking exercises and other similar activities;
e. news or feature articles (or other similar disclosures) about your achievements, awards received, research and public service activities, and the like in UP public spaces, publications, websites or social media posts, or disclosures that UP may make in the exercise of its sound discretion in response to inquiries from the press, or press releases and other similar disclosures for journalistic purposes, as allowed by the DPA, or with your consent;
f. disclosure of relevant personal data in relation to selection processes for certain posts, when such personal data is made available online, pursuant to the principle of democratic participation, and in the interest of transparency;
g. publishing, broadcasting, transmitting, uploading or streaming of UP activities or events pursuant to the legitimate interests of UP or third parties, or for journalistic purposes as allowed by the DPA;
h. disclosures needed in order to enable UP to deposit salaries and other compensation directly to an employee's bank account;
i. information that we share with third parties who process your information in order to provide products or services to you or UP (e.g. to enable the printing of your UP ID card, cloud service providers for data processing systems, email and software providers, third party health providers and medical laboratories that process your medical clearance, and annual physical examinations). Unless your consent is given, it will not be possible for such products or services to be provided to you;
j. disclosures needed in order to enable you to receive medical treatment from third party health providers in the event you are physically or legally unable to give consent;
k. disclosures made pursuant to law and lawful issuances or orders of public authorities, such as the Civil Service Commission, Government Service Insurance System, PhilHealth, Home Development Mutual Fund, Commission on Higher Education, Commission on Audit, law enforcement agencies, courts, and quasi-judicial bodies;
l. disclosures made in order to respond to valid Freedom of Information requests;
m. disclosures made in order for UP to respond to an emergency and comply with its duty to exercise due diligence to prevent harm or injury to you or others;
n. disclosures to establish, exercise, or defend legal claims; and
o. such other disclosures that may be made pursuant to the DPA and other applicable laws.

Where applicable, UP will take reasonable steps to require third parties who receive your personal data to uphold your right to data privacy.

V. RETENTION OF YOUR PERSONAL DATA

UP shall retain and provide measures for the secure storage of your personal data for as long as the above purposes for processing such data subsist, in order to establish or defend legal claims, or as otherwise allowed or required by the DPA and other applicable laws and issuances. UP will archive and provide for the secure disposal of your personal data pursuant to the requirements of, among other laws and issuances, the DPA, National Privacy Commission issuances, National Archives Act, Commission on Audit issuances and Civil Service Commission Memorandum Circulars No. 8, Series of 2007, and No. 1, Series of 2011.

VI. HOW UP PROTECTS YOUR PERSONAL DATA

UP has put in place physical, organizational and technical measures to protect your right to privacy and is committed to reviewing and improving the same. From time to time UP posts information on relevant sites and sends emails that explain how you can secure and maintain the confidentiality of your personal data.

UP System and CU offices are permitted by the DPA and other laws to share information with each other for the purpose of carrying out the mandate of UP pursuant to the Constitution, UP's Charter and other applicable laws. For example, appointments of certain personnel require that their personal data be transmitted by the recommending unit to other CU offices (HRDO, Budget Office, Accounting Office), and by their CU to the UP Board of Regents, through channels. Rest assured that UP officials and personnel in such offices are allowed to process your personal information only when such processing is part of their official duties.

VII. ACCESS TO AND CORRECTION OF YOUR PERSONAL DATA AND YOUR RIGHTS UNDER THE DPA

You have the right to access personal data being processed by UP about you. You may access your personal information, for instance, where applicable through the Human Resources Information System (HRIS) or request documents from relevant offices (e.g., the relevant Human Resources Development Office, Accounting Office). In order for UP to see to it that your personal data is disclosed only to you, these offices will require the presentation of your UP ID, or other valid government-issued IDs (GIID), and documents that will enable such offices to verify your identity. In case you process or request documents through a representative, in order to protect your privacy, we require you to provide a letter of authorization specifying the purpose for the request of documents or the processing of information, and your UP ID or other valid GIIDs, as well as the valid GIID of your representative.

In the event that your information needs to be corrected please follow the instructions found in the relevant website or kindly get in touch with the proper UP office(s).

Aside from the right to access and correct your personal data, you have the following rights subject to the conditions and limitations provided under the DPA and other applicable laws and regulations:

a. The right to be informed about the processing of your personal data through, for example, this and other applicable privacy notices.
b. The right to object to the processing of your personal data, to suspend, withdraw or order the blocking, removal or destruction thereof from our filing system. Please note however that (as mentioned above) there are various instances when the processing of personal data you have provided to us is necessary for us to comply with UP's mandate, statutory and regulatory requirements, or is processed using a lawful basis other than consent. In the case of your UP RFID card it is your duty to immediately report the loss of such card to the proper HRDO and the UP ITDC so that UP can prevent the unauthorized use of the same.
c. The right to receive, pursuant to a valid decision, damages due to the inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data, considering any violation of your rights and freedoms as a data subject; and
d. The right to lodge a complaint before the National Privacy Commission provided that you first exhaust administrative remedies by filing a request with the proper offices or a complaint with the proper Data Protection Officer (DPO) through the email address indicated below regarding the processing of your information or the handling of your requests for access, correction, blocking of the processing of your personal data, and the like.

VIII. HOW WE OBTAIN YOUR CONSENT AND HOW YOU CAN WITHDRAW CONSENT

UP obtains your consent for the processing of your personal data pursuant to this privacy notice by asking you to sign the relevant form or, in some instances, to give your consent through electronic means. If you wish to withdraw consent, please write or send an email to the relevant UP office that processes your information and identify the processing activity for which you are withdrawing consent. Please provide a copy of your UP ID or other GIID so that the relevant office will be able to verify your identity. Note that consent may be withdrawn only for a processing activity for which consent is the only applicable lawful ground for such processing. Please await the responsible office's action regarding your request. Rest assured that once such office confirms that you have validly withdrawn consent for a processing activity the same shall be effective unless you thereafter send a letter or email to said office with a copy of your ID that you are consenting to such processing activity.

IX. REVISIONS TO THIS PRIVACY NOTICE AND QUERIES REGARDING DATA PRIVACY

We encourage you to visit the site where this notice is posted from time to time to see revisions to this privacy notice. We will alert you regarding changes to this notice through this site.

CU personnel who have data privacy queries or concerns regarding the processing of their personal data may contact the UP (insert CU) Data Protection Officer through the following:

a. Via post
b. Through the following landlines

c. Through email

For queries, concerns, comments or suggestions regarding this System-wide privacy notice, as well as data privacy queries or concerns of UP System personnel regarding the processing of their personal data, please contact the University of the Philippines System Data Protection Officer through the following:

a. Via post

c/o the Office of the President
2F North Wing Quezon Hall
(Admin Building) University Avenue,
UP Diliman, Quezon City 1101
Philippines

b. Through the following landlines

Phone | (632) 9280110; (632) 9818500 loc. 2521

c. Through email

dpo@up.edu.ph