REVISED PRIVACY NOTICE FOR UNIVERSITY OF THE PHILIPPINES PERSONNEL AS OF ACADEMIC YEAR 2025-2026

POLICY

The University of the Philippines (UP) is committed to comply with the Philippine Data Privacy Act of 2012 (DPA) https://www.officialgazette.gov.ph/2012/08/15/republic-act-no-10173/ in order to uphold your right to data privacy.

This privacy notice explains in general terms:

(1) the nature, purpose/(s) and extent of the processing of your personal data;

(2) the legal basis/(es) for such processing;

(3) the risks associated with such processing and the measures that UP has put in place to protect your data privacy rights; and

(4) your data privacy rights and how you may exercise the same.

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

The terms UP/University/us refer to the University of the Philippines System and its Constituent Universities (CU), any of its offices, or any of its officials or authorized personnel.

For the sole purpose of this notice, the terms you/your/University personnel refer to past and present UP employees, as well as non-employees engaged by UP to perform services pursuant to contract including, for example, lecturers, visiting professors, professors emeriti, etc.

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

PERSONAL DATA COLLECTED AND PROCESSED

In the course of your employment or engagement with UP, you accomplish, sign and submit forms prescribed by law or lawful issuances of public authorities (e.g., Civil Service Commission [CSC] Personal Data Sheet (PDS) with Work Experience Sheet (WES), Statement of Assets and Liabilities and Net Worth [SALN], Government Service Insurance System [GSIS], PhilHealth, Home Development Mutual Fund [HDMF or Pag-IBIG] forms) or file applications in connection with your employment or engagement

(application for renewal of appointment or tenure for academic staff, leaves, privileges or benefits etc.). In the case of certain appointments, a copy of your PDS with WES, will be transmitted to the CSC and you are required under CSC issuances to authorize the CSC as well as UP, through their authorized representatives to verify or validate all the information contained in your PDS with WES. We also require you to submit documents containing your personal data in compliance with laws, rules and regulations. For instance, CSC issuances require us to securely store in your 201 file, among others, a copy of your scholastic or academic record, medical certificate and the results of relevant pre employment medical examinations, your birth certificate authenticated by the Philippine Statistics Authority (PSA) or relevant Local Civil Registrar (LCR), marriage certificate (if applicable) authenticated by the PSA or proper LCR, valid National Bureau of Investigation clearance and your abovementioned latest PDS. In the case of non employees who render services pursuant to a contract of service or job order, UP processes your personal data pursuant to the requirements of applicable laws, rules and regulations issued by public authorities including but not limited to the Bureau of Internal Revenue, Civil Service Commission, Commission on Audit, Department of Budgement and Management, Government Procurement Policy Board etc.

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 and/or recordings of proceedings and the like containing your personal data. Your personal data may also be included in documents, records, publications, research, minutes and/or recordings produced by other UP personnel tasked with documenting UP meetings, training activities and events.

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 pursuant to its legitimate interests. In the course of operating such CCTV systems, UP may capture your images.

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

UP may also collect publicly available information about you as allowed by the DPA.

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

- **Personal Details**: Name, addresses (e.g. residential, permanent, etc.), personal email address and any UP mail address or any other email address that will be issued or has been issued to you by UP, other contact information, your birthdate, age, birthplace, sex assigned at birth as indicated in your Philippine Statistics Authority (PSA) birth certificate, civil status, religion, citizenship, whether you are a member of an indigenous people's group, suffer from any disability, are a solo parent pursuant to the requirement of existing laws and regulations, signature and such other information found in your CSC Personal Data Sheet (PDS) that you are required to submit in compliance with CSC requirements, name of father, mother, spouse, children and other family members as required by, for example, GSIS forms or for providing benefits to dependents, personal data contained in your SALN;

- **Educational Background:** Official Transcript of Records or True Copy of Grades, Diplomas, Educational Attainment, etc.;

- **Eligibility/Possible Grounds for Disqualification under existing laws rules and regulations:** CSC PDS requires you, for instance, to indicate if you have CSC eligibility, are a Board/Bar passer and the like and requires you to answer questions regarding whether you are related to the appointing authority, have been criminally charged, convicted of a crime, administratively charged, have been a candidate within the last year for any national or local election (except barangay elections), resigned from government service within 3 months prior to the last elections in order to campaign for a national or local candidate, and if you are an immigrant of another country or acquired permanent residence in another country, etc.

- **Government-Issued Identification**: GSIS Number (Common Reference Number and Business Partner Number), taxpayer identification number (TIN), PhilHealth Number, Pag-IBIG Fund (HDMF) Number, UP employee number, senior citizen or person with disability number, PhilSys ID number etc.;

- **Health information**: height, weight, medical certificate and the results of relevant pre employment medical examinations required by CSC issuances as stated above, etc.

- **Relevant Work Experience and References:** Names, contact details of references, details regarding your prior work experience(s), if any, the information you provide in the CSC prescribed PDS and Work Experience Sheet and other similar information;

- **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 data 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. The CSC PDS for example requires your photograph and thumbmark

PURPOSES FOR THE PROCESSING OF PERSONAL DATA

UP processes your personal data for the following purposes:

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, including verification of your access credentials for UP data processing systems or portals;
3) To verify the information you have provided in your application papers, CSC PDS and WES as required by applicable CSC issuances. Note that the CSC form which you signed and submitted in relation to your appointment for a UP post required you to grant UP authority to verify information in your PDS and WES;
4) To facilitate your employment or engagement, which includes processing your pre-appointment requirements, including as applicable, your medical clearance;
5) 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.
6) 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 other similar third parties ;
7) To communicate with you regarding matters related to your employment or engagement and other legitimate concerns;
8) To create/issue, modify and cancel/delete vehicle stickers or passes, clearances or access to UP's information and communications technology (ICT) based or paper based data processing systems, including email as well as data centers;
9) To maintain employment records or records of your contract(s), as required by law;
10) To assess your performance and competencies;
11) To provide you with available training and development opportunities beneficial to you and UP;

12) To process, when applicable, your applications for grants, scholarships, fellowships, travel authorities, attendance in seminars, conferences and other similar applications for benefits or privileges including those which may apply to your dependent(s) in the case of qualified personnel;
13) To process payments, allowances, and other benefits, and make direct deposits of such applicable payments to your bank account;
14) 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 e.g. GSIS, Philhealth, Home Development Mutual Fund and the like, processing of your Statement of Assets, Liabilities and Net Worth (SALN);
15) To provide, facilitate or manage health and other welfare-related services, when available, to qualified personnel and their dependents, subject to UP's rules;
16) To comply with internal processes and legal requirements in the administration of disciplinary proceedings;
17) To investigate and resolve work-related incidents;
18) To provide a safe workplace, and secure UP premises from threats, theft, robbery, fraud, legal liability, and similar incidents;
19) To manage the assets and documents that may have been released to you in the course of your employment or engagement with UP;
20) To process the disbursement of expenses that may have been incurred by you in the performance of your functions when applicable;
21) To process any certifications, or any other documents that you may request from UP in relation to your employment or engagement;
22) To establish a contact point in the event of an emergency involving you, your colleagues, or third parties;
23) To comply with the obligations stipulated in your employment or engagement contract;
24) To conduct audits, or investigate a complaint or security threat;
25) When so required, to process the termination of your employment or engagement;
26) When so required, to settle accountabilities upon termination of your employment or engagement;
27) 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;
28) To enable you to participate, where applicable, in selection processes, such as for the selection of the Faculty or Staff Regent, and the like;
29) 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 above mentioned 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 valid or 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.

30) Other analogous cases/situations deemed proper and legal by UP

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

DISCLOSURES

Examples when UP discloses personal data as allowed by the DPA or other applicable laws, include:

a. disclosures done by the University in the exercise of its academic freedom;
b. 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;
c. 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;
d. 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;

e. disclosures in order to enable UP to participate in university ranking exercises and other similar activities;
f. 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;
g. 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;
h. publishing, broadcasting, transmitting, uploading or streaming of UP activities or events pursuant to the legitimate interests of UP and or third parties, or for journalistic purposes as allowed by the DPA;
i. disclosures needed in order to enable UP to deposit salaries and other compensation directly to an employee's bank account in a government depositary bank as required by applicable laws, rules and regulations;
j. information that we share with third parties who process your information in order to provide products or services to you and/or UP (e.g. to enable the printing of your UP ID card, cloud service providers for data processing systems, email and software providers, any third party health providers and medical laboratories that process your medical clearance, and annual physical examinations).
k. 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;
l. 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;
m. disclosures made in order to respond to valid Freedom of Information requests;
n. 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;
o. disclosures to establish, exercise, or defend legal claims; and
p. 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 comply with the requirements of the DPA and National Privacy Commission issuances as well as other applicable laws, rules and regulations and uphold your right to data privacy.

OUR LAWFUL BASES FOR PROCESSING YOUR PERSONAL DATA

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 and legal obligations to you and to pursue its legitimate interests.

NPC Advisory Opinion 2022-14 https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No.-2022-014_Redacted.pdf provides that

> ***Processing of personal data within the educational framework in relation to academic freedom.***
>
> At this juncture, the NPC would like to clarify that educational institutions may process personal data to achieve the purposes within its educational framework without the need for consent of the data subject. The data subject in an educational setting includes students, faculty and staff. It is then of utmost importance that the school delineates all processing operations, carefully identifying those that are core to the educational framework and those outside of it (e.g. marketing or public relations purposes).
>
> x x x
>
> … the NPC respects the same doctrine of Academic Freedom for the processing of personal data within the educational framework, if it is in accordance with the provisions of the DPA and other existing laws, rules and regulations. The NPC will remain neutral on the chosen methods and technology by the educational institution as long as it is within the bounds of the law (footnotes omitted, underscoring supplied).

You may wish to refer to the case of Garcia vs. Faculty Admissions Committee Loyola School of Theology G.R. No. L-40779 November 28, 1975 68 SCRA 277 (1975) cited in University of the Philippines vs. Arokiaswamy G.R. No. 134625. August 31, 1999 https://elibrary.judiciary.gov.ph/thebookshelf/showdocs/1/3688 which states that:

> Wide indeed is the sphere of autonomy granted to institutions of higher learning, for the constitutional grant of academic freedom, to quote again from *Garcia v. Faculty Admission Committee, Loyola School of Theology,* "is not to be construed in a niggardly manner or in a grudging fashion (footnotes omitted,underscoring supplied)."

Please also note that 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.

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. See for example, the CSC Omnibus Rules on Appointments and Other Human Resource Actions. 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, the National Archives Act, National Privacy Commission, Commission on Audit, Civil Service Commission and National Archives of the Philippines issuances.

UP will also store your personal data pursuant to Sec. 11 (f) of the DPA which states Provided, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.

UP conducts research on stored, previously processed, de-identified data in order to comply with its legal obligations including its right and responsibility to exercise academic freedom under the 1987 Constitution and the UP Charter. UP as a research university must conduct scientific research in order to produce general demographic information and statistics regarding UP personnel across various time periods. Such research enables the University to assess whether its policies, programs, as well as procedures and revisions to the same in different years, enable the University, among others, to comply with its Charter and other applicable laws, rules and regulations.

Before any research is conducted by UP, so that we will be able to comply with our ethical obligations and uphold your right to privacy, duly authorized UP personnel will remove identifiers from the applicable dataset such that UP's researcher or research teams who will perform operations on such dataset will not be able to associate your data with you. The research results will only include aggregate or statistical data and general demographic information that does not identify you and any other data subjects.

Kindly note that Sec. 16.C.2 of Memorandum Circular 2023-4 issued by the National Privacy Commission provides that:

> "The conduct of research where the end results will be anonymized and will only disclose the general demographic of the research subjects does not require the consent of the data subject."

On the other hand, if research will make use of identifiable personal data, when so required by applicable laws, rules and or ethical guidelines such as the guidelines issued by the Philippine Health Research Ethics Board pursuant to the Philippine National Health Research System Act, we will first obtain the proper ethics clearance as well as your informed consent prior to the conduct of such research.

DATA PRIVACY RISKS AND HOW UP PROTECTS YOUR PERSONAL DATA

The processing by UP of your personal data carries risks that may involve the confidentiality, integrity, and availability of personal data or the risk that processing will violate the privacy principles and rights of data subjects. UP has put in place reasonable physical (e.g. access control measures such as locks, security personnel, etc.) organizational (e.g. only authorized personnel who have signed the required non-disclosure undertaking and need such personal data to perform their functions are allowed to process such personal data, periodic privacy impact assessments etc.) and technical measures (e.g. use of CDN, encryption, multi factor authentication for UP mail and use of SSO via UP mail for portals, the conduct of vulnerability and penetration testing and other similar measures) to prevent or mitigate such risks. Kindly note that

these measures do not guarantee absolute protection against such risks as when systems are subject to targeted cyber attacks, malware, ransomware, computer viruses, etc. However, UP has also adopted measures in order to deal with security incidents or personal data breaches in compliance with the DPA and National Privacy Commission (NPC) issuances.

Please refer to the Board of Regents approved UP Data Privacy Manual CERTIFIED_TRUE_COPY_DATA_PRIVACY_MANUAL_2023_EDITION.pdf (up.edu.ph) which includes security incident and breach response procedures (Part 7) and the following forms:

Form 1 UNIVERSITY OF THE PHILIPPINES SYSTEM ADMINISTRATION INCIDENT OR BREACH REPORT FORM.docx (up.edu.ph)

Form 2 PRELIMINARY ASSESSMENT FORM FOR SECURITY INCIDENTS OR PERSONAL DATA BREACHES (up.edu.ph)

Form 3 Mandatory Notification to NPC.pdf (up.edu.ph)

Form 4 Mandatory Personal Data Breach Notification for Data Subjects.docx (up.edu.ph)

Form 5 SECURITY INCIDENT OR PERSONAL DATA BREACH REPORT (up.edu.ph)

We remind UP offices, officials and personnel in our various portals, privacy notices and security advisories transmitted by our IT offices to keep the processing of personal data secure by double checking that the UP mail account used for UPs portals and systems has not been compromised by using Have I Been Pwned, using a strong password for such account 2023_12_04_REMINDER_–_Use_Strong_Passwords_for_UP_Mail_Accounts and 2025_06_20_REMINDER_Strong_Passwords_UPMail keeping all UP account credentials confidential, using when possible more stringent means for multi factor authentication (MFA) for UP mail accounts such as through the use of passkeys or hardware based MFA and not using public, unsecured networks for processing personal data or at least using VPN if use of such unsecured networks is unavoidable and periodically provide other similar advisories as well as trainings.

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 data, for instance, where applicable through UPs online

processing systems or portals or request documents from relevant offices (e.g. PUSO, the relevant Human Resources Development Office, Accounting Office, etc.). In order for UP to see to it that your personal data is disclosed only to you or when you exercise any of your data privacy rights (see your other data privacy rights below), the relevant UP office processing your personal data will require the presentation of your UP ID, or other valid government-issued IDs (GIID), and documents that will enable such office to verify your identity. In case you request documents or exercise your data privacy rights through a representative, in order to protect your privacy, such relevant UP office processing your personal data will require you to provide a letter of authorization specifying the purpose for the request of documents or the processing of information or the right(s) you wish to exercise and the data processing system(s) or application(s) to which your request refers and your UP ID or other valid GIIDs, as well as the valid GIID of your representative and such other documents that may be used in order to verify your respective identities and the basis/es for the exercise of your data privacy rights as provided under Sec. 18 of the UP System Data Privacy Manual.

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) 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.

HOW WE OBTAIN YOUR CONSENT AND HOW YOU CAN WITHDRAW CONSENT

As explained above, in most instances, UP processes your personal data pursuant to its exercise of academic freedom such that per the NPC Advisory Opinion 2022-14 https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No.-2022-014_Redacted.pdf, there is no further need for UP to obtain your consent for such processing. In instances when consent is the appropriate basis for processing, UP obtains your consent by asking you to sign the relevant form or, in some instances, to give your consent through electronic means. If you are below eighteen years of age, we will require your parent or guardian to execute or sign and submit the proper consent form or withdrawal of consent letter.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 subject to limitations provided by law as well as contractual obligations and 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.

REVISIONS TO THIS PRIVACY NOTICE AND QUERIES REGARDING DATA PRIVACY

This privacy notice was revised as of Academic Year 2025-2026 in order for UP to comply with the privacy notice requirements in NPC MC 2023-4 and to inform UP personnel of NPC Advisory Opinion 2022-14 https://privacy.gov.ph/wp-content/uploads/2022/08/Advisory-Opinion-No.-2022-014_Redacted.pdf. The privacy notice and consent form covered by Memorandum TJH 2019-25 dated 18 October 2019 have been superseded by this revised privacy notice.

We encourage you to visit the UP Privacy site https://privacy.up.edu.ph/ where this notice is posted from time to time to see any 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 their respective CU UP Data Protection Officer through the following:

a. Via post
b. Through the following landlines
c. Through email

UP Diliman

Post: Lower Ground Floor, PHIVOLCS Building.
C.P. Garcia Avenue
Diliman, Quezon City 1101

Landline: 8255-3561

Email: dpo.updiliman@up.edu.ph

UP Los Baños

Post: Office of the University Registrar, G/F CAS Annex I Building, UP Los Baños, College 4031, Laguna, Philippines

Landlines: (049) 536-2553 / (049) 536-2426

Email: dpo.uplb@up.edu.ph

UP Manila

Post: 3/F Information Technology Center, Joaquin Gonzales Compound, University of the Philippines Manila, Padre Faura St., Ermita, Manila

Landline: +63 (2) 509-1003; (PGH) 554-8400

Email: dpo.upmanila@up.edu.ph

UP Visayas

Post: c/o Office of the University Registrar
New Administration Building,
University of the Philippines Visayas
5023 Miag-ao, Iloilo

Landline: (033) 315-9631 or 315-9632 and local numbers 191-192

Email: dpo.upvisayas@up.edu.ph

UP Open University

Post: 2/F UP Open University Main Building
UP Open University Los Banos 4031 Laguna

Landlines: (049) 536-6001 to 006 local 299

Email: dpo.upou@up.edu.ph

UP Mindanao

Post: c/o Office of the Chancellor
University of the Philippines Mindanao
Barangay Mintal, Davao City 8022

Landline: (082) 293-0310

Email: dataprotection.upmindanao@up.edu.ph

UP Baguio

Post: Office of the University Registrar, UP Baguio, Gov. Pack Road, Baguio City 2600

Landline: +63 (74) 445-0785 (HRDO)

Email: dpo.upbaguio@up.edu.ph

UP Cebu

Post: Room 242, Arts and Science building, UP Cebu Lahug Campus

Landline: +63 (32) 233-8203 loc 202

Email: dpo.upcebu@up.edu.ph

For queries, 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