University of the Philippines Diliman
Data Protection Team

upd.edu.ph/privacy
dpo.updiliman@up.edu.ph
(632) 8255-3561

11 November 2019

MEMORANDUM

Reference No. EBM 19-02

FOR	:	Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons
SUBJECT	:	**UP Diliman Privacy Manual**

The UP Diliman Privacy Management Program Framework under Data Protection Officer Memorandum No. EBM 19-01 envisions to nurture a culture of respect for privacy. Part of the threefold approach to implement this vision is to *"Develop privacy by design through promulgation of sound policies, leveraging technologies, and proactive planning"*. To this end, a privacy manual for UP Diliman should be sufficiently robust to steer units and offices into a unified direction yet sufficiently utilitarian and flexible to act as an enabling catalyst for privacy maturity.

In line with the UP Diliman Data Protection Officer's responsibility under Office of the Chancellor Memorandum No. 19-073 to issue data privacy policies, the attached UP Diliman Privacy Manual is hereby promulgated.

Elson B. Manahan, JD
Data Protection Officer

Noted by:

Michael L. Tan, DVM, PhD
Chancellor

University of the Philippines Diliman

PRIVACY MANUAL

Chapter I.
INTRODUCTION

The University of the Philippines Diliman ("UP Diliman") adopts this Privacy Manual to cultivate conscientiousness in respecting data privacy rights through adherence to the general principles of transparency, legitimate purpose, and proportionality as well as the enforcement of data security measures.

Chapter II.
SCOPE AND EFFECTIVITY

This Manual governs the acts and decisions of all types of students, parents, guardians, faculty, visiting faculty, staff, Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, retirees, applicant students, applicant faculty, applicant staff, researchers, research subjects, patients, clients, customers, alumni, donors, donees, contract counterparties, partners, subcontractors, outsourcees, licensors, licensees and other persons whose personal data are directly or indirectly processed by UP Diliman (collectively referred to as "UP People").

The provisions of this Manual are effective on the date of its promulgation until revoked or amended by the Data Protection Officer.

Chapter III.
PROCESSING OF PERSONAL DATA

UP Diliman, its academic units and its administrative offices process personal data in pursuance of the University's mandates under the laws and issuances, as an educational and research institution, and as an instrumentality of the government.

(A) Grounds and purposes of processing personal data

The basis of UP Diliman's processing of personal data may be one or more of the following grounds:

(1) Performance of its obligations, exercise its rights, and conduct its associated functions as:
    (a) an instrumentality of the government;
    (b) a higher education institution.
(2) Pursuance of its purposes and mandates:

(a) under Act No. 1870 as "a university for the Philippine Islands";
(b) under Republic Act 9500 as "the national university".

(3) For each particular unit of UP Diliman, conducting all acts reasonably foreseeable from and customarily performed by similar bodies;
(4) Deciding and acting for the holistic welfare of its students, their parents and guardians, faculty, staff, researchers, alumni, and UP Diliman community; and
(5) Managing and administering its internal and external affairs as an academic and research institution, as an instrumentality of the government, and as a juridical entity with its own rights and interests.

Based on one or more of the above-mentioned grounds, UP Diliman processes personal data to achieve the following purposes:

(1) Academic, research, extra-curricular, student welfare and disciplinary purposes;
(2) Supervision of academic and researchers endeavors;
(3) Management of human resources and supervision of work conduct;
(4) Student and employee application processing and identity verification purposes;
(5) Documentation and record-keeping purposes;
(6) Medical, physical, psychiatric and psychological attention purposes;
(7) Alumni linkage, donation and funding purposes;
(8) Customer, client, patient or community service purposes;
(9) Contractual and financial purposes;
(10) Corporate governance and housekeeping, regulatory and audit purposes.

The UP Diliman General Privacy Notice found in the UP Diliman Website is the fundamental notice to the public how UP Diliman processes personal data. Specific privacy notices may exist for particular initiatives, projects and endeavors that involves data processing.

(B) Types of personal data processed

Types of personal data processed by UP Diliman are:

(1) Personal details such as name, birth, gender, civil status and affiliations;
(2) Contact information such as address, email, mobile and telephone numbers;
(3) Academic information such as grades, course and academic standing;
(4) Employment information such as government-issued numbers, position and functions;
(5) Applicant information such as academic background and previous employments;
(6) Medical information such as physical, psychiatric and psychological information.

(C) Data Classification

Data may either be restricted (internal, confidential, or sensitive confidential) or publicly available. All documents and files in UP Diliman either in physical or electronic format must be classified into one of the categories below. If needed, a section in a document or a file may be given a classification different from the document or file containing it. Privacy Focal

Persons have the obligation to ensure that documents and files owned or primarily managed by their respective UP Diliman unit or office have proper data classifications.

Data restrictions

Access to data in UP Diliman are restricted to varying *classes of users* according to risk level:

1. Internal – Data which generally pose a **low risk**.
2. Confidential – Data which generally pose a **medium risk**.
3. Sensitive Confidential – Data which generally pose a **high risk**.

(1) Internal

Definition: Data which should be internally contained within certain UP Diliman units or offices.

Restriction: May be accessed only by UP Diliman units or offices which need such data to perform their roles and responsibilities.

Risk: Low. UP Diliman may incur financial losses, reputational damage, or lose opportunities.

Examples:

- Employee benefits may be accessed by HRDO and Accounting Office but not by unconcerned offices.
- Draft documents not yet cleared for release may not be demanded by other offices.

(2) Confidential

Definition: Information which in may only be disclosed only to a limited number of individuals to protect UP Diliman from legal, regulatory, financial, strategic, operational or reputational risks.

Restriction: May be accessed only by UP Diliman officials, staff or faculty if the data is necessary to perform an official task.

Risk: Medium. UP Diliman may be incur judicial or administrative liability. Rights of individuals may be violated.

Examples:

- Personal information such as home address, email, and photos.
- Patent application documents.

(3) Sensitive Confidential

Definition: Information that may likely cause serious harm to UP Diliman or individuals if not strictly protected.

Restriction: May be accessed on a need-to-know basis only by the minimum number of UP Diliman officials, staff or faculty whose knowledge of the information is highly necessary to address a need.

Examples:

- Sensitive personal information such as age, political affiliation, health, education, and government-issued I.D. numbers.
- Privileged information such as those in sexual harassment cases disclosed to officials, adjudicators, lawyers and doctors.

Public data

Public data should be freely accessible to parties internal and external to UP Diliman. Except for reasonable procedural requirements, there should be no restrictions to access public data.

The UP Diliman Freedom of Information Manual should be complied with in requests invoking the freedom of information.

(D) Frameworks and periods in processing personal data

UP Diliman processes personal data in accordance with the parameters and periods provided by the following:

(1) The Data Privacy Act of 2012, its Implementing Rules, and relevant issuances of the National Privacy Commission;
(2) The National Archives of the Philippines Act of 2007 its Implementing Rules, and relevant issuances of the National Archives of the Philippines;
(3) The UP Diliman Privacy Management Program Framework;
(4) Policies, guidelines, and rules of the UP System and UP Diliman;
(5) Research guidelines and ethical codes of conduct adopted by the University of the Philippines Diliman;
(6) Executive Order No. 2, series of 2016 on Freedom of Information and subsequent related executive orders;
(7) Laws or regulations which amend or repeal the foregoing.

Chapter IV.
SECURITY MEASURES

UP People are mandated to implement the following security measures in all actions and decisions directly and indirectly related to processing of personal data:

(A) Organizational Security Measures

(1) Data Protection Officer and Privacy Focal Persons

The protection of personal data flowing, within, and out of UP Diliman's units and offices are under the autonomous and independent jurisdiction and authority of the UP Diliman Data Protection Officer. Each academic unit and administrative office of UP Diliman shall appoint a Privacy Focal Person to support the Data Protection Officer and implement privacy and security initiatives for the unit or office concerned.

(2) Roles in the Protection of Personal Data

The Data Protection Officer has the responsibility to:

- Comply with legal and regulatory obligations related to data privacy;
- Provide data protection support to various units and offices;
- Enforce UP Diliman's policies related to data privacy, information security, records management and data governance;
- Coordinate with relevant offices to strengthen organizational, physical and technical security measures; and
- Supervise Privacy Focal Persons in the ensuring data privacy across UP Diliman.

Privacy Focal Persons have the responsibility to:

- Support the Data Protection Officer's endeavors and initiatives;
- Implement privacy policies and initiatives;
- Proactively prevent, monitor, mitigate and manage existing or reasonably foreseeable security incidents and personal data breaches in their respective units;
- Strictly observe the UP Diliman Security Incident Management Policy; and
- Investigate, address, remediate and resolve privacy gaps, and if necessary, impose sanctions to erring UP People in their units.

The Data Protection Officer may promulgate policies, rules and guidelines related to data privacy, information security and records management.

(3) Pillars of Accountability and Compliance

The heads of UP Diliman academic units and administrative offices shall ensure that their unit has appointed a Privacy Focal Person under Office of the Chancellor Memorandum No. MLT-18-022.

Privacy Focal Persons shall conduct a Privacy Impact Assessment for UP Diliman units and offices under the guidance and supervision of the Data Protection Team.

The Data Protection Officer shall implement a framework for an integrated and holistic privacy management program for UP Diliman.

The Data Protection Team and Privacy Focal Persons shall implement privacy and data protection measures through policies, initiatives and remedial measures to effect non-disruptive, collaborative and enabling change toward data protection.

The UP Diliman-level Breach Response Team and the Unit-level Breach Response Teams shall be responsible for security incident and personal data breach management and notification by following the procedure of the UP Diliman Security Incident Management Policy in Office of the Chancellor Memorandum No. MLT-18-072.

(4) Education

The Data Protection Team shall conduct Records Management and Data Privacy Capacity Building Seminars to all academic units and administrative offices of UP Diliman as mandated by Office of the Chancellor Memorandum No. MLT-18-256.

For UP People regularly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations, as often as necessary.

(5) Privacy Impact Assessment

Privacy Focal Persons shall conduct a Privacy Impact Assessment (PIA) of their units relative to all activities, projects and systems involving the processing of personal data. This shall be done under the guidance and supervision of the Data Protection Team. The PIA shall include an assessment of the documents, data processing systems and policies of UP Diliman units and offices. The PIA shall include the process of understanding the personal data flow, identifying and assessing threats and vulnerabilities, and proposing measures to address privacy risks.

(6) Privacy Principles

In all actions and decisions involving personal data, UP People shall ensure that the following privacy principles are applied:

- *Transparency.* The individual must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
- *Legitimate purpose.* The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
- *Proportionality.* The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

(7) Oversight and Review

The oversight and review of privacy initiatives are in UP Diliman Oversight and Review Plan which:

- Sets measures in ensuring that the policies and procedures for data privacy are followed and updated;
- Defines roles and responsibilities of academic units and administrative offices in the oversight and review of UP Diliman's policies and initiatives; and
- Identifies which Generally Accepted Privacy Principles UP Diliman shall utilize to review its overall privacy management program.

(B) Physical Security Measures

(1) Format of data to be collected

Personal data collected by UP Diliman may be in digital/electronic format or paper-based/physical format.

(2) Storage type and location

The physical storage locations of personal data are folders, envelopes drawers, cabinets, rooms, vaults and other file storage devices and locations within the premises of UP Diliman or in storage facilities contracted by UP Diliman. At all times, storage locations not in use shall be kept secure and locked. Storage devices such as external hard disks, USB flash disks and optical disks should be kept secure in locked storage location when not in use.

Privacy Focal Persons shall lead the implementation of the UP Diliman Records Management Policy in their respective units and offices.

(3) Access procedure of agency personnel

Only authorized UP People shall be allowed to enter or access storage locations, facilities and devices containing personal data. Other personnel may be granted access upon approval of the Data Protection Officer upon request of the head and the Privacy Focal Person of the concerned UP Diliman unit or office.

(4) Monitoring and limitation of access to room or facility

Access to documents and files containing personal data shall be restricted to UP People that have the appropriate security clearance. Efforts to create an access control system to record when, where, and by whom data centers are accessed.

Preferably, UP People authorized to access paper-based or physical storage locations must register with a paper-based or electronic registration platform of UP Diliman before accessing any document or file. They shall indicate the date, time, duration and purpose of each access.

Drawers, cabinets, rooms and other storage locations containing personal data must be kept closed and locked when not in use or when not attended. Keys for these storage locations must at all times be kept secure.

Privacy Focal Persons shall lead the implementation of the UP Diliman Organizational and Physical Data Protection Measures Policy in their respective units and offices.

(5) Configuration and design of workspaces

As much as practicable (1) machines and workspaces will be positioned in consideration of privacy and the protection of the processing of personal data; and (2) workspaces shall be configured and designed to restrict documents, files and screens from the view of those who are not assigned to the concerned workspace.

Printouts containing personal data should be immediately removed from printers.

(6) Clean Desk Policy

Documents containing personal data should not be (1) exposed in desks and other work places as soon as they are no longer in use; (2) left in desks during breaks, when an errand will be done out of the immediate workspace, or when it is the end of the workday (3) outside of designated storage places at the end of the day and when the individuals concerned are expected to be gone for an extended period.

UP People should regularly allocate time to clear away paperwork on desks.

(7) Limitation of view and copies of documents

UP People shall not display or work on personal data in public view. Documents and files with personal data shall be kept away when there is a visitor or guest near the workspace and not have copies or reproductions more than minimally necessary.

(8) Duties and responsibilities of UP People

In all acts and forms of processing of personal data, UP People shall at all times:

- Maintain confidentiality and integrity of personal data;
- Comply with all organizational, physical and security measures required by UP Diliman and data privacy regulations;
- Process personal data compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy;
- Process personal data when proportionate, necessary and not excessive in relation to a declared and specified purpose;
- Ensure that the rights of the data subject are not violated;
- In applicable cases, obtain the consent of data subjects;
- Comply with the UP Diliman Privacy Policy; and
- Observe the UP Diliman Data Subject Rights and Responsibilities.

(9) Disclosure or transfer of personal data within UP Diliman or to external parties

Physical disclosure or transfer of documents containing personal data shall be conducted by UP People whose work functions include the transmission or delivery of the concerned document when related to a legitimate purpose of the concerned UP Diliman unit or office. In case of special circumstances wherein the work functions of the individual involved do not

include the transmission or delivery of the document, then the approval of the Privacy Focal Person having jurisdiction is necessary.

(10) Retention and disposal procedure

Excessive copies of documents should be disposed in a manner that prohibits reconstruction of the data therein, such as disposal by shredding.

UP Diliman processes and retains personal data in accordance with the "Frameworks and periods in processing personal data" in this Manual.

In the absence of an applicable rule of retention or disposal, a UP Diliman unit may act in accordance with the practices of government bodies with analogous functions.

A document and excessive copies thereof must be disposed in a manner that prevents reconstruction of the data therein (such as shredding) if all the following requisites are present:

(1) There is no law or regulation requiring the continued use or retention of the document;
(2) UP Diliman has no foreseeable indispensable need for the document; and
(3) No data subject rights will be violated.

(C) Technical Security Measures

(1) Collection and storage of electronic information

Digital information are stored in hardware and cloud locations either under the possession or control of UP System or UP Diliman. The storage and related functions on personal data may be outsourced upon execution of an Outsourcing Agreement in accordance with data privacy laws, rules and issuances.

(2) Monitoring for security breaches

As needed, each UP Diliman unit or office shall determine and use technologies not falling below industry standards and practices in the academe necessary to prevent any attempt to interrupt or disrupt data processing systems.

(3) Security features of the software used

Prior to their installation and use, application software and system software used should be reviewed and evaluated by the appropriate information technology personnel of the concerned UP Diliman unit or office before the installation thereof in computers and devices. Compatibility of security features with overall operations must also be ensured by these personnel. In case of lack of relevant personnel or expertise, the UP Diliman Computer Center must be consulted prior to use of any software.

(4) Process for testing, assessment and evaluation of effectiveness of security measures

The UP Diliman Oversight and Review Plan shall serve as the primary guide in monitoring, assessing, revising and reporting the effectiveness of privacy endeavors and programs.

The appropriate information technology personnel shall review security policies, conduct vulnerability assessments and perform penetration testing within the of the concerned UP Diliman unit or office.

(5) Security measures that control and limit access to personal data

Personal data in rest, in transit and in use must at all times maintain their confidentiality, integrity and availability through compliance with the UP Diliman Information Security Policy, the implementation of which should be led by Privacy Focal Persons.

Personal data that are digitally processed are preferably encrypted, whether at rest or in transit. An appropriate encryption minimum standard (such as Advanced Encryption Standard with a key size of 256 bits (AES-256) or its predecessor technology) is preferred. Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. Passwords and passphrases should at least be a minimum of twelve (12) characters. The UP Diliman Computer Center shall ensure password and passphrase policies are at par with security best practices.

Transfers of personal data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments.

Use of facsimile technology is not secure and hence it should not be used for transmitting documents containing personal data.

The data processing systems which process personal data must be included in UP Diliman's Privacy Impact Assessments as well as the UP Diliman Oversight and Review Plan.

Personal data may only be accessed online or remotely by UP People unless there is a legitimate purpose to disclosure personal data to external parties as approved by the concerned Privacy Focal Person.

UP People who access personal data online or remotely shall authenticate their identity via a secure encrypted link and must use multi-factor authentication. Their access rights must be defined and controlled by a system management tool.

As much as practicable, UP Diliman, its units and its offices shall adopt and utilize technologies that prevent personal data accessible online from being copied to a local machine. Preferably, there is automatic deletion of temporary files that may be stored on a local machine by its operating system.

Preferably and as much as practicable, the saving of files to portable storage devices (such as external hard disks, USB flash disks and optical disks) should be prohibited by UP Diliman units and offices. Drives and USB ports on local machines may also be disabled as a security measure. An allocated network drive shall always be preferred to saving files locally to a machine. In case there is a need to save in a local machine or a portable storage device, only UP People and not external parties may access such files. If there is a need to save files in portable storage devices, only official portable devices encrypted with

technologies not falling below industry standards shall be used with the consent of the concerned Privacy Focal Person.

Chapter V.
BREACH AND SECURITY INCIDENTS

The mitigation, management and resolution of Security Incidents and Personal Data Breaches requires the coordination of various UP People. All concerned should be vigilant in their responsibilities to enable an effective security incident management process.

(i) Data Breach Response Teams

UP Diliman Breach Response Teams (BRTs) are an organized group of Staff mandated to assess and evaluate Security Incidents, which includes Personal Data Breaches, restore integrity to the information and communications systems, mitigate and remedy resulting damages, and comply with reportorial requirements. BRTs are under the jurisdiction and authority of the UP Diliman Data Protection Officer.

UP Diliman shall have a Constituent University-level Breach Response Team (the "Diliman-Level BRT") and a Breach Response Team for each academic unit and administrative office (the "Unit-Level BRT").

BRTs shall be responsible of the following:

- Implementation of the Security Incident Management Policy of UP Diliman;
- Management of Security Incidents and Personal Data Breaches; and
- Compliance with the relevant provisions of the Data Privacy Act of 2012, its Implementing Rules and Regulations, and all related issuances by the National Privacy Commission on Personal Data Breach management.

The teams must be ready to **assess and evaluate** a Security Incident, **restore integrity** to the information and communications system, **mitigate and remedy** any resulting damage, and **comply** with reporting requirements.

The UP Diliman Security Incident and Management Policy establishes the roles and responsibilities of BRTs.

(ii) Measures to prevent and minimize occurrence of breach and security incidents

Privacy Focal Persons should coordinate with the Data Protection Office for the conduct of the Privacy Impact Assessment as needed to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks.

UP People directly involved in the processing of personal data must attend trainings and seminars for capacity building.

UP Diliman units should conduct inventories of information assets. As far as practicable, UP Diliman units should adopt information security policies that address the specific needs of their units with applicable controls and procedures. In no case shall policy specific to a unit may supersede or prevail over UP Diliman's data privacy policies.

There shall be a system to regulate access to data centers owned or controlled by UP Diliman. Appropriate security clearances or access control lists should be set up for classes of administrators and uses. There should be an access control system that records when, where, and by whom the data centers are accessed. Copies of access control lists and similar records must be filed to UP Diliman Data Protection Office.

The UP Diliman Message and Communication Policy should be followed in the creation, sending, transmittal, receipt, access, use, processing, and storage of documents, instruments, files and data in any form or medium containing personal or confidential information.

The UP Diliman Data Protection Guidelines for Work Processes should be observed in all stages of performing functions and tasks directly or indirectly related to UP Diliman.

(iii) Procedure for recovery and restoration of personal data

UP Diliman units and offices shall always maintain a backup for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

As far as practicable, UP Diliman units and offices shall have disaster recovery and continuity plans to ensure availability of data despite the occurrence of disruptions.

(iv) Notification, documentation and reporting protocol

The following incident management and notification procedure is established in the UP Diliman Security Incident Management Policy:

Section A. Incident Response Procedure

- Step 1 – Reporting
- Step 2 – Categorization
- Step 3 – Investigation and Identification

Section B. Breach Notification

- Step 4 – Reporting and Notification

Section C. Mitigation Response Plan

- Step 5 – Containment and Eradication
- Step 6 – Recovery

- Step 7 – Feedback
- Step 8 – Learning

Chapter VI.
INQUIRIES AND COMPLAINTS

Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the UP Diliman, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the UP Diliman at dpo.updiliman@up.edu.ph and briefly discuss the inquiry, together with their contact details for reference.

Complaints shall be filed in three (3) legible printed copies, or sent to dpo.updiliman@up.edu.ph. The Data Protection Officer may instruct the concerned office or unit shall confirm with the complainant its receipt of the complaint. The Data Protection Officer may instruct the concerned Privacy Focal Person to shall liaise with all necessary third parties, including dealing with the complainant.

Chapter VII.
DEFINITION OF TERMS

"Data Protection Officer" is the official of the University of the Philippines Diliman who has independent and autonomous jurisdiction and authority over data protection and privacy matters.

"Personal data" refers to personal information, sensitive personal information or privileged information as defined by the Data Piracy Act of 2012 or any subsequent law. Personal information is information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.

"Processing" refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

"UP Diliman" refers to the University of the Philippines Diliman, an autonomous constituent university of the University of the Philippines System.

"UP People" refers to all types of students, parents, guardians, faculty, visiting faculty, staff, Research, Extension and Professional Staff (REPS), UP contractual personnel, Non-UP contractual personnel, retirees, applicant students, applicant faculty, applicant staff, researchers, research subjects, patients, clients, customers, alumni, donors, donees, contract counterparties, partners, subcontractors, outsourcees, licensors, licensees and other persons whose personal data are directly or indirectly processed by UP Diliman.