Data Protection Office

upd.edu.ph/privacy

dpo.updiliman@up.edu.ph

(632) 8255-3561

22 July 2020

MEMORANDUM

UPD DPO Memorandum No. EBM

i. ***Units and Offices*** refer to University of the Philippines Diliman academic units and administrative offices;

j. ***UP Diliman*** refers to the University of the Philippines Diliman;

k. ***UP People*** refers to 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 with a juridical link with UP Diliman.

II. Organizational Security Measures

Section 4. *Data Access* Access to a particular type of data shall be determined based on its classification under the UP Diliman Data Classification Policy.[3]

Access to any data owned by UP Diliman shall only be granted to authorized UP People with a legitimate purpose for the same. Furthermore, they must refrain from gaining unauthorized access or exceeding the authorized access to the data granted to them.

In accessing the data, the concerned UP People must maintain the quality and integrity of the same.

Units and offices providing access to the data in their custody must ensure that proper access controls, such as access logs, are maintained to document the movement of the data.

Section 5. *Data Collection* The data collected by UP People must not be excessive for the legitimate purpose for which it was intended.

Thus, prior to providing any requested data, it is incumbent upon the concerned UP People to determine if the request is for a legitimate purpose and not contrary to any rules and regulations promulgated by UP Diliman.

Section 6. The use of data shall only be granted to authorized UP People with a legitimate purpose for the same. Consequently, any disclosure or transfer of data must be only in the pursuance of their official functions.

All UP People using the data must use the same strictly for its intended purpose only. Furthermore, they must refrain from performing any act that would amount to the unauthorized use of the data or exceeding the authorized use of the same. In using the data, the concerned UP People must likewise ensure that the quality and integrity of the same is preserved.

Furthermore, copyright, licenses, and intellectual property rights must be observed and respected in the course of the use of the data. Thus, users are strictly enjoined to not infringe on the copyright and other property rights covering the data that is the subject of their use.

In addition thereto, all UP People accessing and/or using data within the premises of UP Diliman through its computing facilities, networks and other information technology

[3] *See* Note 1

resources are enjoined to abide by the Acceptable Use Policy for Information Technology Resources of the UP System.[4]

Units and offices providing access to the data in their custody must ensure that proper usage controls, such as logs, are maintained to document the movement of the data.

Section 7. *Privacy* All UP People accessing and processing data must do so under strict confidentiality, in order to ensure that any internal, confidential, or sensitive confidential information will not be disclosed to unauthorized persons.

Section 8. *Privacy Focal Persons* Privacy Focal Persons are designated by the Office of the Chancellor to coordinate and assist the UP Diliman Data Protection Team in its endeavors; implement privacy policies and initiatives; monitor, mitigate, and manage foreseeable security incidents and personal data breaches in their respective units and offices; and investigate, address, and resolve privacy gaps in their respective units and offices.[5]

Section 9. *Messages and Communications* UP People creating, sending, transmitting, receiving, accessing, using, processing, and storing messages and communications, whether in print or electronic format, must ensure that the private information therein is maintained and kept confidential. Furthermore, they must ensure that the same will be for the intendent parties therein only.

Section 10. *Consent to the Processing of Personal and Private Information* The processing of any personal or private information shall require the consent of the data subject.

In crafting consent notices or forms, the right of the data subject to be informed and create an intelligible decision must be of paramount importance.

Section 11. *Responsibility of UP People* Acts and decisions of UP People with respect to any information that they process in relation to their dealings with UP Diliman must be in line with the UP Diliman Privacy Manual.[6]

Moreover, in the conduct of their affairs, UP People are to abide by the three cardinal principles of privacy to ensure that data is at all times protected:

a. ***Transparency*** Data subjects to be informed of the nature, purpose, and extent of the processing of their personal data;
b. ***Legitimate Purpose*** The data must be processed only for the purpose for which it was intended, provided that the same is not contrary to laws, morals, and public policy. Moreover, the consent for the processing must be freely given by the data subject;

Section 12. *Security Incidents* In the event of a security incident or data breach, units and offices must abide by the guidelines provided in the UP Diliman Security Incident Management Policy.[7]

III. Physical Security Measures

Section 13. *Data Format* Data accessed, collected, and processed, whether in print or electronic format, must be kept secure by all UP People concerned.

Section 14. *Storage* Data storage devices such as, but not limited to, folders, envelopes, drawers, filing cabinets, vaults, rooms are kept within the premises of UP Diliman and/or storage facilities contracted by UP Diliman.

Section 15. *Storage Access* Access to the data storage facilities shall be subject to the following restrictions:

a. Only authorized UP People are allowed to enter the premises where data is kept.

c. *Water* Computing assets and storage devices must be placed in a location safe from water damage. If the unit or office is situated in an area prone to flood, it is advisable that the assets or devices be stored in a remote site instead.

Units and offices must ensure that -47(o)-(e)-p(3)-47(a)7(d)-(a)-(d)adit lmo-69ni.