University of the Philippines

Proposed University Data Privacy Policy

Version 0.02
27 February 2014

Table of Contents

Preamble

The University of the Philippines respects the privacy of all, regardless of race, color, gender, or religious, political, philosophical, or organizational affiliation. In this Digital Age, information has also transcended into a commodity which may have economic value. The University prohibits unlawful distribution of and/or access to data in its possession, through any of its various offices, units, educational institutions, and externally contracted parties. Republic Act 10173, otherwise known as the Data Privacy Act of 2012, embodies the spirit of this law, and Chapter II, Section 7(f) specifies "[Coordination] with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country," hence this Policy.

I. Policy Statement and Summary

A. The University of the Philippines (henceforth "University") is committed to protecting the fundamental human right of privacy and of communication while ensuring the free flow of information and the right level of transparency to the Public. Under this principle, the University shall adhere to the related laws in force.

B. The University, meanwhile, needs to collect, store, process, and retrieve certain personal information about its faculty, staff, students, and/or clients, partners, contractors and other such service providers to carry out its daily operations, meet its objectives, fulfill its mandate, or otherwise comply with legal obligations and/or requirements.

C. The University recognizes the need to treat these data in an appropriate and lawful manner in line with Republic Act No. 10173, otherwise known as the "Data Privacy Act of 2012" or other laws related or repealing the same. In respect of all personal and/or private data it handles, the University ensures that all information collected will be used fairly, stored safely, and not disclosed to any other individual or organization unlawfully.

D. Towards this end, the University:

1. May be required to manage a variety of types of information which include details of its past, current, and prospective faculty, staff, students, and/or clients, partners, contractors and other such service providers;
2. Is subject to certain legal requirements specified in the Data Privacy Act of 2012 and other related laws in force regarding the information for which it handles, which may be held on paper, digitally, or any other media; and
3. Provides for disciplinary action, including and up to the appropriate legal remedy, should any breach of this Policy occur.

II. Scope

A. General Coverage

1. This policy shall apply to all faculty, staff, and students of the University and all other clients, partners, contractors and other such service providers affiliated with the University.
2. This policy shall likewise cover the use and contents of University owned, leased, rented, or on-loan facilities which collect, store, process, and retrieve certain personal information; private systems, whether they are owned, leased, rented, or on-loan when used to perform actions stated above; to all University-

owned/licensed data/programs, be they on University or on private systems; and to all data or programs provided to the University by sponsors or external agencies.

3. All users must be aware of the regulations and understand that they are bound by this Policy when performing actions that meet the stipulations outlined above.

B. Local Use

1. Units within the University may provide for additional terms of use, guidelines, restrictions, enforcement mechanisms, and any other such conditions for personnel, devices, data, program, equipment, or any other apparatus under their jurisdiction which collect, store, process, and retrieve certain personal information.
2. When adopting additional regulations, units will be responsible for publishing such conditions regarding the appropriate and/or authorized use of the information for which they are responsible.
3. Provided, however, that such additional regulations is consistent with the overall policy explicitly stated in this Policy.

III. Definition of Terms

For the purposes of this Policy, the following terms are defined, to wit:

a. *Consent of the data subject* refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. Consent shall be evidenced by written, electronic, or recorded means. It may also be given on behalf of the data subject by an agent specifically authorized by the data subject to do so.
b. *Data subject* refers to an individual whose personal information is processed.
c. *Personal information* refers to any 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.
d. *Personal information controller* refers to a person or organization who controls the collection, holding, processing, or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:
    i. A person or organization who performs such functions as instructed by another person or organization; and
    ii. An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.
e. *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, deletion, or destruction of data.

IV. Purpose of the Policy

This Policy aims to:

A. Set out rules and regulations on data protection and the legal conditions, obligations, and requirements that must be satisfied with regard to the collection, storage, processing, and retrieval of certain personal information;
B. Ensure all relevant stakeholders that those responsible in handling personal data are fully aware of any such requirements in accordance with data privacy and protection procedures;
C. Prescribe mechanisms that help identify and prevent the compromise of personal data and the misuse of such;
D. Ensure the automation, technical support, and implementation of proper guidelines needed to keep this Policy effective;
E. Define mechanisms that protect the reputation of the University with respect to its data privacy and protection procedures;
F. Implement best practices in addressing the following data privacy and protection principles, which include, but are not limited to personal data that are:
    1. Obtained, processed, and retrieved legally;
    2. Specified, explicit, and lawful purposes of data collection;
    3. Used and disclosed to other parties in ways legally and compatible with the principles and mandate of the University;
    4. Stored safely and securely;
    5. Maintained complete, accurate, and updated at all times; and
    6. Adequate, relevant, and retained not longer than for the purpose(s) for which it was collected, processed, stored, and retrieved; provided consistent with the laws in force related to retention of Government information.

V. Policies

A. Obtained, Processed, and Retrieved Fairly

The following shall be the minimum guidelines for collecting and processing personal data and any other such private information:

1. Obtaining Personal Information

   The Data Privacy Act of 2012 does not inhibit or otherwise prevent the collection and processing of personal and private data, but ensures however that process is done fairly and without compromising the right(s) of the data subject.

2. Processing Personal Information

   The data subject must be told who the data processor will be, for specified and legitimate purposes determined and declared beforehand, or as soon as reasonably applicable after collection, and later processed in a way which fulfill such declared, specified, and legitimate purposes.

3. Legal Conditions

   For personal data to be processed lawfully, certain legal requirements have to be met. This includes, among other things, the subject explicitly consenting to the collection and processing of personal information, or that the data is necessary for

the legitimate interest of the data processor or the party to whom the data will be of use.

B. Specified, Explicit, and Lawful Purposes for Data Collection

The following shall be the minimum guidelines for the purposes of collecting and processing personal data and any other such private information:

1. Purpose of Data Collection
   Personal information may only be processed for the specific and legitimate purpose(s) as notified to the subject when the data was first collected or as soon as reasonably allowed.

2. Change of Data Collection Purpose
   If it otherwise becomes necessary or legitimate to change the purpose for which the data was collected, the subject must be informed of the new purpose before any processing is to occur.

3. Data Collection for Other Purposes
   Should there be a need to collect personal information for other purposes, the University will inform the data subject of such matters when and where it is appropriate and should obtain consent for such collection and processing.

C. Used and Disclosed to Other Parties in Ways Compatible with such Purposes

The following shall be the additional conditions when disclosing personal data to other parties for legitimate, official, and lawful purposes:

1. Use of Data Collected
   Personal data should only be collected and processed to the extent that is required and necessary for the specific and legitimate purpose notified to the data subject. Any other such data, which is not necessary for that purpose, should not be collected in the first place.

2. Accountability and Responsibilities of External Parties
   External parties shall be responsible for lawfully disclosed University information under its jurisdiction, control, or custody, including information that have been transferred/given to it by external agencies for processing.

   They shall likewise provide a comparable level of protection while such information are under their jurisdiction, control, or custody, and designate an individual or individuals accountable for the information collected and processed in compliance with this policy. The identity of the individual(s) so designated shall be made known to the data subject upon request.

D. Stored Safely and Securely

The University shall ensure that appropriate security measures are taken against unlawful or unauthorized collection and processing or personal data, as well as against the

accidental loss, damage, unlawful and fraudulent access, misuse, and unlawful destruction, alteration, and contamination of such information.

1. Confidentiality
   Only individual(s) who are authorized to use the data must be given access to it. The University will ensure that only authorized personnel will have access to a data subject's personal information and any other private or sensitive data held by the same.

2. Integrity
   The personal data obtained and processed shall at all times be accurate and suitable for the purpose for which it was collected and processed.

3. Availability
   Authorized users should be able to access the data should the need arise for official, legitimate, and specified purposes.

4. Security of Personal Data
   The University shall likewise employ reasonable, appropriate and lawful organizational, physical, and technical measures intended for the protection of personal information. Subject to other policies applicable to the handling and management of personal data, security measures must, at the very least, also include:
   a. Safeguards to protect computer network(s) and other electronic medium against accidental, unlawful, and unauthorized access, usage, and interference with personal data;
   b. A protocol for identifying reasonably foreseeable vulnerabilities in the University's computer networks, and for taking preventive, corrective, and mitigating action against such incidents that may otherwise lead to a security breach; and
   c. The regular monitoring of such possible security breaches.

E. Maintained Complete, Accurate, and Updated
The following are guidelines to ensure the accuracy and completeness of personal data obtained and processed:

3. Accurate and Complete Data
   Personal data must be kept accurate and complete at all times. In line with this, the University shall take the necessary and appropriate actions to ensure that information which are incomplete, misleading, or otherwise inaccurate are checked and verified at regular intervals.

4. Data Correction Procedures
   Should relevant change(s) to one's personal data occur, it shall be the responsibility of the data subject to provide the University with the updated version of the concerned personnel's information (e.g., change of address, contact

number, or marital status). In this regard, the University may grant the data subject access that could allow limited modification of the stored data.

F. Retained Not Longer for Its Purpose

Personal data must not be kept longer than is necessary for its intended and original purpose. The University, however, has certain legal obligations to keep certain types of information only for some specified period of time. In addition, the University may at time need to retain personal data for a period of time to protect its legitimate interests.

VI. Rights of the Data Subject

The data subject is entitled to:

A. Request access to data being held about them by a personal information controller;

B. Be informed whether personal information pertaining to him or her shall be, are being, or have been processed;

C. Ask to have inaccurate data amended;

D. Prevent the processing of information that is likely to cause damage or distress unto the data subject or those around him or her; and

E. Be furnished with the following at the most reasonable time:
   1. Description of the personal information obtained or processed;
   2. Purpose(s) for which they are being, or are to be, used for, collected and/or processed;
   3. The individual(s) or organization(s) to which such information may be disclosed;
   4. The period for which the data may be stored;
   5. The existence of these rights.

VII. Subject Access Request

A formal request from a data subject for information that the University holds about them must be made in writing. Data subjects should be provided their data in accordance with any such request within thirty (30) days of submitting the request.

VIII. Penalties

For students and personnel within the University, the enforcement guidelines of the University Acceptable Use Policy shall apply. Otherwise, for contracted external parties, sanctions for policy violations shall be met with the appropriate legal remedies in accordance with Sections 25-37, Chapter VIII, of the Data Privacy Act of 2012.