University of the Philippines Diliman

FAQs in filling out the PIA Questionnaire

Frequently Asked Questions (FAQs) in accomplishing the Privacy Impact Assessment (PIA) Questionnaire

In compliance with National Privacy Commission Advisory No. 2017-03, all **Privacy Focal Persons** in UP Diliman appointed under Office of the Chancellor Memorandum No. MLT-18-135 are requested to conduct a Privacy Impact Assessment (PIA) of their UP Diliman academic unit or administrative office by accomplishing the UP Diliman PIA Questionnaire which is attached in the email sent with this document.

What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment (PIA) is the self-assessment that the National Privacy Commission mandated for personal information controllers such as UP Diliman. The objectives of the PIA are to determine how an organization processes personal information, identify the privacy risks, and manage these risks. The PIA identifies, keeps track, and evaluates the various stages of personal data processing to identify and remediate gaps in its Data Life Cycle.

In UP Diliman, our primary tool for a Privacy Focal Person's PIA of his/her unit is the PIA Questionnaire which is divided into three (3) spreadsheets: Documents, Policies and Data Processing Systems.

How do I accomplish the "Documents" spreadsheet?

1. List down all Documents managed your UPD unit.

   "Documents" are form, template, record, list, table, report, issuance, invoice, receipt or other documents that contain personal information of individuals. Examples are enrollment forms, class lists, request forms, approval forms, vouchers, etc.

2. For each document, identify information on the *processing* of the concerned document (inbound, outbound, storage, final status).

3. For each document, identify *data privacy* information in the concerned document (personal information, sensitive information, disclosures, excessiveness).

   a. *Personal information* are any information that can be used to ascertain the identity of an individual. Examples are name, student number, age, contact information, etc.

   b. *Sensitive information* are those information which may cause material damage if misused. Examples are educational information, health information, financial information, etc.

4. Still in the Documents spreadsheet, tell us if you need data privacy help by identifying problems in the concerned document (security, useless steps in processing, risks in processing, etc.).

    a. *Processing* refers to any act done in the document, including accomplishing, receiving, storing, transferring using, disclosing, sharing or destroying the information in the document or the document itself.

5. Tell us your suggestions, if any, on how to improve the concerned document.

Do not hesitate to consult relevant people in your unit to identify and understand the documents used by your unit.

How do I accomplish the "Policies" spreadsheet?

1. In the Policies spreadsheet, list down the title of all the Policies in your UPD units which relates to data governance, data privacy or information security.

    For this purpose, policies includes approved rules, regulations, procedures, guidelines, manual, memo, circular or order in your UPD unit.

2. For each policy, write down the involved UPD units whom are required to follow and those having jurisdiction or authority in cases of violation.

3. Still in the Policies spreadsheet, tell us if you need data privacy help by identifying matters or items that need to be included or revised to improve data privacy.

4. Tell us your suggestions, if any, on what other policies we should create.

How do I accomplish the "Data Processing Systems" Spreadsheet?

1. In the Data Processing Systems spreadsheet, list down the name of the Data Processing Systems your unit or sub-unit use.

    Data Processing Systems refers to either computerized system or physical records which stores, processes or transmits personal information or sensitive personal information owned or managed by your UP Diliman unit or office

    Note: Do not include systems or records managed by another unit or office.

2. For each Data Processing System, identify what classes of UP people's information are being processed.

    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.

3. For each Data Processing System, what other UP units or Non-UP offices that can access the personal information or sensitive personal information.

4. For each Data Processing System, list down the type of access that other UP units or Non-UP Offices they have (admin/ edit/ view) in the system.

5. Still in the Data Processing Systems spreadsheet, write down the office/s or person/s that receive report with personal information from the system or record.

6. List down the data privacy or information security measures that are currently used to protect data, that are missing or features that are unnecessary.

7. Still in the Data Processing Systems spreadsheet, tell us if you need data privacy help by identifying vulnerabilities, threats or risks to the system or record that should be addressed.

8. Tell us your suggestions on what other improvements, if any, that we can make to the system or record.

What are examples of Personal Information?

Personal information refers to information that can reasonably and directly ascertains an individual or when put together with other information would directly and certainly identify an individual, like:

- Personal details such as name;
- Contact information such as address, email, mobile and telephone numbers.

What are examples of Sensitive Personal Information?

These refers to information that may be used to damage or discriminate against individuals such as:

- Individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- Academic information such as grades, course and academic standing;
- Employment information such as government-issued numbers, position and functions;
- Applicant information such as academic background and previous employments;
- Medical information such as physical, psychiatric and psychological information.

What are some examples of Organizational, Physical and Technical Security Measures?

It is the duty of UP Diliman to implement reasonable and appropriate organizational, physical and technical security measures for the protection of personal data. Below are some examples:

Organizational Security

- Trainings and seminars about Data Privacy and Security
- Privacy Impact Assessment

Physical Security

- Secured storage type and location
- Authorized personnel to access the data storage facility
- Monitoring and limitation of access to data storage facility
- Implementation of Clean Desk Policy

Technical Security

- Implementation of Password policy
- Identification using multi-level authentication