ADVISORY NO. 18-03

Developing Privacy Policies

Background

Under Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), a person generally has the right to be informed that his or her personal data is being or is about to be processed by an organization, group, or another person. Additional details about such processing must also be provided. This is consistent with the general principle of transparency in data processing, and also supports such data privacy principles as fairness, purpose specification, openness, and accountability.

To uphold this right, an organization, group, or person engaged in data processing develops and uses a Privacy Policy (i.e., Privacy Notice, Privacy Statement, etc.).

The Ateneo de Manila University, through the University Data Protection Office (UDPO) and with the assistance of various units and offices, has developed Privacy Policies addressing its four (4) principal stakeholders: students, personnel, and visitors—both online and offline. They are now all available at the UDPO website.

Unfortunately, these four Policies will not always cover the data processing systems and activities being managed or carried out by the University, through its many different units and offices. There will be times when specific units or offices, their programs or projects, or new data processing systems will require separate and distinct Privacy Policies. This makes it important for units and offices to be capable of drafting their respective Policies, with little to no supervision necessary.

For these reasons, the UDPO now issues these guidelines for the development of Privacy Policies.

1. Scope

This Advisory applies to existing or new data processing systems owned, managed, or controlled by the University, through its various units and offices, including individual personnel who carry out such a task in their official capacity.

Adherence to this Advisory only ensures compliance with provisions of the DPA, its Implementing Rules and Regulations (IRR), and other applicable issuances of the National Privacy Commission (NPC). Compliance concerns vis-à-vis other data protection laws (i.e., European Union’s General Data Protection Regulation) must be referred to the UDPO.
2. Definitions

Whenever used in this Advisory, the following terms shall have their respective meanings as set forth herein:

2.1. “Consent” refers to any freely given, specific, informed indication of will, whereby an individual agrees to the collection and processing of his or her personal data. There must be a written, electronic, or recorded proof of such consent.

2.2. “Control” refers to the authority to dictate or determine the manner, method, or terms under which personal data may or shall be processed.

2.3. “Data processing system” refers to any process or procedure by which personal data is collected, used, or otherwise processed in an information and communications system, or at least a filing system.

2.4. “Data Subject” refers to the individual whose personal data is being processed.

2.5. “Personal Data” refers to the collective term used for personal information, sensitive personal information, and privileged information. It does not include aggregate or anonymized data.

2.6. “Personal Information” refers to any information, on its own or when combined with other information, from which the identity of an individual is apparent or can be reasonably and directly determined.

2.7. “Privileged Information” refers to all forms of data, which the Rules of Court and other laws consider to be privileged communication.

2.8. “Process Owner” refers to the unit, office, center, or individual personnel of the University who controls or maintains a data processing system.

2.9. “Processing” refers to any operation performed on personal data including, but not limited to, collection, recording, organization, storage, updating, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data.

2.10. “Public Authorities” refer to any government entity with law enforcement or regulatory authority or function, as vested by law or the Constitution.

2.11. “Sensitive Personal Information” refers to personal information:

- about a person’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- about a person’s health, education, genetic or sexual life, or to any proceeding for any offense he or she committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings;
- issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
- specifically established by an executive order or an act of Congress to be kept classified.

2.12. “University” refers to the Ateneo de Manila University, including its units, offices, centers, institutes, and laboratories.
3. General Principles for Processing Personal Data

Processing of personal data by the University shall observe the general principles of transparency, legitimate purpose, and proportionality.

3.1 Transparency. An individual should be informed of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, his or her rights as a data subject, and the manner by which these rights can be exercised.

3.2 Legitimate purpose. Data processing systems and activities must have a legitimate purpose. It should be consistent with the mandate of the University and should not be contrary to law, public morals, or public policy.

3.3 Proportionality. Data processing systems and activities, including the amount and types of data involved, and the period within which they are kept, should be relevant, necessary, and not excessive in relation to their declared and specified purpose.

4. Data Privacy Principles

Processing of personal data by the University shall also be guided by the data privacy principles.

4.1 Purpose Specification and Limitation. Personal data should be collected for specified and legitimate purposes, and must only be processed in a way that is compatible with such purposes.

4.2 Lawfulness and Fairness. Personal data should be processed in accordance with the law and in a transparent manner.

4.3 Data Quality. Whenever possible, personal data should be kept accurate, relevant, and up to date.

4.4 Collection Limitation. The amount of data collected should not be excessive in relation to the purpose or purposes of their collection.

4.5 Retention Limitation. Unless otherwise permitted by law, personal data should only be retained as long as they are necessary for the fulfillment of the purposes for which they were collected.

4.6 Secure Further Processing. Personal data collected for other purposes may be processed for historical, statistical, or scientific purposes. In some cases, retaining them for longer periods may be allowed by law, as long as adequate safeguards are in place.

5. Legal Bases for Processing

Processing of personal data by the University shall always be supported by appropriate legal bases.

5.1. In the case of Personal Information, any or all of the following may be valid ground for processing:

5.1.1. The data subject must have given his or her consent.
5.1.2. Processing is necessary in relation to a contract between the University and the data subject.

5.1.3. Processing is necessary for the University to comply with a legal obligation.

5.1.4. Processing is necessary for the University to protect vitally important interests of the data subject, including his or her life and health.

5.1.5. Processing is necessary for the University to respond to a national emergency or to comply with the requirements of public order and safety, as prescribed by law.

5.1.6. Processing is necessary for the University, or a third party, to pursue its legitimate interests, unless such interests are overridden by the fundamental rights and freedoms of the data subject.

5.2. In the case of Sensitive Personal Information and Privileged Information, any or all of the following may be valid ground for processing:

5.2.1. The data subject must have given his or her consent. In the case of privileged information, both parties must have given their consent.

5.2.2. Processing is authorized by law or regulations that guarantee the protection of personal data.

5.2.3. Processing is necessary to protect the life and health of the data subject or another person. However, the data subject must not be able to legally or physically express his or her consent prior to the processing.

5.2.4. Processing is necessary to provide the data subject with medical treatment to be carried out by a medical practitioner or medical institution that has adequate level of data protection.

5.2.5. Processing is necessary to protect the lawful rights and interests persons in court proceedings.

5.2.6. Processing is necessary to establish, exercise, or defend a legal claim.

5.2.7. Personal data is to be provided to the government or a public authority, in accordance with the latter’s constitutional or statutory mandate.

6. General Guidelines

A unit or office planning to develop a Privacy Policy must keep in mind the following:

6.1. Preliminary Matters

Determine first if there is a need to draft a Privacy Policy. For this purpose, three key questions must be considered:

6.1.1. What types of data are being processed? Only when personal data are involved will data protection laws and policies apply, including the requirement for a Privacy Policy.
6.1.2. What types of personal data are being processed? If personal data are involved, identify the type/s included, i.e., personal information, sensitive personal information, or privileged information.

6.1.3. What are the legal bases for the data processing? Once the types of data involved have been ascertained, determine the specific section of the law (see: Sections 12 and 13, DPA) that is applicable to the processing of those types of data. One may also refer to Section 5 above. After all legal bases have been properly identified, one can ascertain if a Privacy Policy is sufficient, or if a Consent Form will also be necessary.

Data processing activities that are justified only by the consent of an individual will require the development of an appropriate Consent Form. If consent is not required by law and there are other legal bases for the processing, a Privacy Policy is enough. For this reason, it is important to note that a Privacy Policy is different from a Consent Form, even though the latter will always contain the former.

A separate UDPO Advisory will feature the guidelines for drafting proper consent forms.

6.2. Elements

A proper Privacy Policy must answer the following questions:

6.2.1. Who is the Personal Information Controller (PIC)? The PIC controls the processing of personal data. In the context of the University, it is the University that is the PIC. For Policies developed by a specific unit or office, identifying that unit or office in the document is also recommended.

6.2.2. What data are being collected or generated? It is not necessary to specify every single data point (e.g., name, age, ID number, etc.). The classification or categories of the personal data involved is sufficient (e.g., directory information, educational records, etc.).

6.2.3. What is the purpose of the processing? Consistent with the purpose specification and limitation principle, it is important to indicate what the collected data will be used for. Compatible uses such as research, and other uses permitted by law may also be mentioned.

6.2.4. Who has access to the data? Among the information an individual is entitled to is the identity or category of persons who gets to access his or her personal data. If the University will allow them to be accessed automatically, and the data subjects have agreed to this, the method for such access should also be discussed.

6.2.5. With whom are the data shared, if at all? If personal data is shared or transferred to persons or organizations separate or distinct from the University, such recipients or classes thereof (e.g., affiliates, subsidiaries, etc.) must also be indicated. Note, though, that sharing or transfer of data is only allowed when required or permitted by law.

6.2.6. How long will the data be retained? Consistent with the retention limitation principle, it is important that personal data be retained only for as long as they are still necessary to the purpose of their collection, or when allowed by law. It is not always necessary to provide a specific unit of time (e.g., 1 year, 5 weeks, etc.). What is important is to give the individual concerned an idea of how long his or her data will be kept.
6.3.9. *Statement on data subject rights and on how to exercise them.* An individual must be informed of the existence of his or her rights with respect to his or her data. How such rights may be exercised should also be explained briefly.

6.3.10. *Contact Information.* An individual must also be given the contact details of the relevant unit or office of the University to whom he or she may relay a complaint, question, or clarification regarding the processing of his or her personal data. The contact information of the UDPO, as provided below, may also be included:

**University Data Protection Office**
+63 2 426-6001, loc. 4801
info.udpo@ateneo.edu (for inquiries)
alert.udpo@ateneo.edu (for complaints and security incidents)

6.3.11. *Other Information.* Other relevant information that may also be included, such as:

- **How are the data disposed of?** A Policy may explain briefly how collected personal data will be disposed of or deleted after they are no longer necessary or if they have already served their purpose.

- **General statement on security measures.** A Policy may also contain a brief statement regarding the level of security being maintained in order to protect the collected data.

- **Effectivity of updates.** The Policy may indicate how updates or revisions will be relayed to affected individuals and how such updates or revisions will be implemented.

6.3. *Format*

There is no prescribed format for a Privacy Policy, although the following points are worth considering:

6.3.1. *Style and Tone.* The Policy should be delivered in plain and clear language. Translations to different languages or dialects are welcome if the intended audience is comprised of people with diverse linguistic backgrounds. Context is extremely important. Use of humor, art, and even sarcasm, can be effective but only when used appropriately.

6.3.2. *Length.* The Policy should be long enough to include all information prescribed by law, but short and simple enough for an individual to actually read. That said, bigger organizations or more complex processing systems will necessarily entail longer or more elaborate texts.

6.3.3. *Medium.* The delivery of the Policy may be done orally, in written or printed text, via photos or videos, and/or through electronic means. What is important is that the medium deemed most effective in conveying the message to the target audience should be selected. The simultaneous use of multiple media is also possible, if resources will permit.

6.4. *Other Considerations*

6.4.1. *Consultation with stakeholders.* Consultations are invaluable when developing a Privacy Policy. Inputs from process owners will ensure that its content is comprehensive and accurate, and will also help develop buy-in. If consulted,
representatives from the target audience can also help determine the ideal format or method of presentation.

6.4.2. Approval process. A Privacy Policy shall undergo the same approval process as any other policy of the University. Accordingly, University-wide Privacy Policies shall be submitted to the University President for approval. Those that pertain to specific units or offices shall be approved by the head or approving authority of those units or offices. This, notwithstanding, no unit- or office-specific Privacy Policy shall depart from or be inconsistent with the main University Privacy Policies.

6.4.3. Responding to complaints, questions, or clarifications. A unit or office must be familiar with the contents of its Privacy Policy, including those of the University’s. It should be able to respond or act promptly in case there are complaints, questions, or clarifications regarding such Policies. When necessary, a unit or office may seek the assistance of the UDPO in this matter.

7. UDPO Review

Review by the UDPO of a Privacy Policy developed by a unit or office of the University is not mandatory, provided that the provisions of this Advisory are followed carefully. This, however, shall not preclude a unit or office from submitting its Policy to the UDPO for review. For this purpose, a reasonable amount of time must be allotted prior to the date of the Policy’s intended use.

8. Compilation

The previous provision notwithstanding, a copy of all approved Privacy Policies should be submitted to the UDPO for compilation and record purposes, including updates thereto or subsequent versions. These Policies form part of the University’s data protection framework, which is being managed by the UDPO.

Failure to observe these guidelines may result in improper or inaccurate Privacy Policies. That, in turn, may increase the likelihood of your unit or office receiving a complaint from an affected individual or a notification from the National Privacy Commission, regarding your failure to conduct your processing activities in a manner that is consistent with the law.

Should you have questions or require clarification regarding this Advisory or any of these recommendations, you may contact the UDPO at info.udpo@ateneo.edu.

For your guidance.

Sincerely,

JAMAEL A. JACOB
Director

Noted by:

JOSE RAMON T. VILLARIN, S.J.
President