Access to or Sharing of Personal Data within the University

In an organization, offices frequently share or allow access to their data. This is because access to information is often—if not always—critical to their functions and operations. Unfortunately, this also poses significant risks to personal data. Information can get lost, altered, or disclosed to unauthorized parties, sometimes resulting in untold injuries or damages.

Consequently, it is important for organizations to integrate data protection into their respective information systems. This Advisory offers some guidelines to keep in mind when implementing such integration.
ADVISORY NO. 2018-04

Access to or Sharing of Personal Data Within the University

Background

In a typical organization, it is common for units and offices to share or allow access to data under their respective control or custody. This is because, in many cases, having access to certain types of information is critical to their functions and operations. Unfortunately, such practice could also pose significant risks to people, especially if it involves their personal data. Information can get lost, altered, or unnecessarily disclosed to unauthorized parties at any point during the process. That, in turn, could lead to injury or damages on the part of the affected individuals.

Often, the solution has been the introduction of data protection laws—these laws, after all, ensure that data processing is carried out in a safe and secure manner. Here in the Philippines, there is Republic Act No. 10173, or the Data Privacy Act of 2012 (DPA). It upholds the twin policies of the State to protect the fundamental human right to privacy, while ensuring the free flow of information.

The DPA, however, only provides general directives. Organizations require specific guidelines that can help them integrate the DPA into their respective data processing systems, including those that involve access to or sharing of personal data. The task of developing such guidelines is often given to the Data Protection Officer (DPO). In the context of the Ateneo de Manila University, it is the University Data Protection Office (UDPO) that bears that responsibility.

For these reasons, the UDPO now issues these guidelines for allowing access to or sharing of personal data between units and offices of the University.

1. Scope

This Advisory applies to the accessing or sharing of personal data being processed by, or under the control or custody of the University, through any of its units or offices. They include requests to access data made by:

1. another office or unit of the University;
2. an administrator, faculty member, or any other personnel of the University, in his or her official capacity; and
3. a service provider, including a Personal Information Processor.

Access by or sharing with other persons or organizations that do not function as service providers of the University will be taken up in a separate UDPO Advisory. Applicable privacy and data protection laws and policies will govern those transactions in the meantime.
2. Objectives

This Advisory aims to:

2.1. demonstrate the willingness of the University to comply with all applicable privacy and data protection laws and policies; and

2.2. ensure the security and confidentiality of personal data accessed or shared within the University.

3. Definition of Terms

Whenever used in this Advisory, the following terms shall have the definitions provided here:

3.1. “Anonymization” refers to a security measure wherein personal data is stripped of any personally identifiable elements, thereby preventing them from being traced back to a specific individual.

3.2. “Applicable privacy and data protection laws and policies” refer to the DPA, its Implementing Rules and Regulations, issuances by the National Privacy Commission, and other privacy and data protection laws that apply to the data processing activities of the University.

3.3. “Consent” refers to any freely given, specific, and informed indication of will, whereby an individual agrees to the collection and processing of his or her personal data. It must be evidenced by written, electronic or recorded means. It may be given on his or her behalf by his or her authorized representative.

3.4. “Data Subject” refers to an individual whose personal data is being processed by or is under the control or custody of the University.

3.5. “Encryption” refers to the process of encoding a message or information in such a way that only authorized parties can access it.

3.6. “National Privacy Commission” refers to the government agency charged with administering and implementing the DPA.

3.7. “Outsourcing” or refers to an arrangement wherein an individual or organization processes personal data upon the instructions or on behalf of another individual or organization.

3.8. “Personal data” refers to all types of personal information, including sensitive personal information, and privileged information.

3.9. “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 it, or when put together with other information would directly and certainly identify an individual.

3.10. “Personal information controller” or “PIC” refers to a person, organization, or body that controls the processing or use of personal data. The term excludes:

3.16.1. a person, organization, or body that performs such functions as instructed by another person or organization; or
3.16.2. an individual who collects, holds, processes or uses personal information in connection with his or her personal, family, or household affairs.

3.11. “Personal information processor” or “PIP” refers to any person, organization, or body to whom a PIC may outsource, subcontract, or instruct the processing of personal data.

3.12. “Privacy Policy” refers to a document or statement through which a PIC or PIP informs a data subject about the processing of his or her personal data, including some details, in line with the general principle of transparency in data processing.

3.13. “Privileged Information” refers to all data which, under the Rules of Court and other relevant laws, constitute privileged communication.

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

3.15. “Pseudonymization” refers to a security measure applied to personal data wherein personally identifiable elements are replaced by one or more artificial identifiers called pseudonyms or codes. Unlike anonymized data, pseudonymized data can be restored to their original status as personal data, thereby allowing the re-identification of the data subject they pertain to.

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

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

3.17. “Service Provider” refers to any authorized person, organization, or body performing a function or providing a service to or on behalf of the University. A PIP is a specific type of service provider.

3.18. “Units and offices” refer to all component or working units of the University, including schools, offices, centers, institutes, departments, and laboratories. It shall also include service providers.

3.19. “University” refers to the Ateneo de Manila University.

4. General Principles

Access to and sharing of personal data shall be governed by the following general principles:

4.1. **Authorized Processing.** Personal data that will be accessed by or shared with another unit or office of the University must have been collected in accordance with the applicable Privacy Policy of the University, or after the consent of the data subjects concerned has been obtained.
The Privacy Policy or the written consent of the data subjects must state clearly that the data may be accessed by or shared with other units or offices of the University.

4.2. *Legitimate Purpose*. Access to or the sharing of personal data with another unit or office of the University must have a legitimate purpose. This means:

4.2.1. It should be consistent with the mandate of the University as an academic institution, employer, and/or organization.
4.2.2. It should be necessary to or compatible with the function or work of that particular unit, office, or University personnel.
4.2.3. It should not be contrary to law, public morals, or public policy.

4.3. *Data Minimization*. Access to or sharing of personal data must be limited to the minimum amount necessary to accomplish or achieve the declared purpose of such access or sharing.

4.4. *Confidentiality*. Unless public disclosure is authorized under the law, the confidentiality of any personal data that will be accessed or shared must be maintained. This duty remains even after a person’s employment or organization’s engagement by the University ends.

4.5. *Accountability*. A unit or office shall be primarily responsible for the personal data under its control or custody, including those it shares or gives access to.

4.6. *Data Retention and Disposal*. Personal data accessed by or shared with another unit or office, or a University personnel, must only be retained within the period necessary to attain the declared purpose of such access or sharing.

5. Security and Confidentiality of Personal Data

The University is responsible for ensuring the security and confidentiality of all personal data it processes, or is under its control or custody. In line with this, it must adopt and implement reasonable and appropriate organizational, technical, and physical security measures to prevent or avoid any accidental or unlawful destruction, alteration, or disclosure, or unauthorized processing. When giving access to or sharing personal data, this may be achieved through the following:

5.1. *Non-Disclosure Agreements and Standard Confidentiality Clauses*. Only University personnel that have accomplished the Non-Disclosure Agreement (NDA) prescribed by the University shall be allowed access to personal data under the control or custody of the University.

Contracts or agreements entered into with service providers, including PIPs, must feature standard confidentiality clauses, as prescribed by the UDPO. In lieu thereof, a separate Non-Disclosure Agreement (NDA) may also be executed by the parties.

Service providers are responsible for ensuring that their personnel are also subject to a similar confidentiality obligation, particularly those who may gain access to personal data shared by the University.

5.2. *Access Restrictions*. Personnel, including those of service providers, shall only be allowed access to personal data necessary or relevant to the performance of their work or function. Every unit or office must establish a clear access restriction policy and a procedure for the issuance of appropriate security clearances.

5.3. *Encryption and Password-Protection*. Secure communications and/or media should be used when accessing or sharing personal data. Whenever possible, information sharing done via
electronic or digital means must be secured through the use of encryption technology, passwords, two-step authentication, and/or other similar tools.

5.4. **Retention Period.** Each unit or office must enforce a data retention schedule that will govern the storage or retention of personal data obtained directly from an individual or from another unit or office of the University. It must provide the conditions for erasure or disposal of the personal data.

Personal data processed for statistical or scientific purposes may be stored for longer periods, provided that data protection measures are in place to secure the data. Anonymized or aggregate data may be retained indefinitely. Those processed for historical and archiving purposes may be stored in accordance with applicable laws and policies.

5.5. **Safe and Secure Disposal.** Where applicable, shared personal data must be returned, disposed of, deleted, or destroyed in a safe and secure manner. The method used must prevent further use or processing of the data.

5.6. **Anonymization, Pseudonymization, and Use of Aggregate Data.** Whenever possible, only data that have been anonymized, pseudonymized, or aggregated should be retained for a period longer than necessary for the declared purpose of their collection.

5.7. **Standard Data Protection Clauses, and Data Protection Covenants.** Where the processing of personal data, in part or as a whole, will be outsourced, subcontracted, or delegated to a service provider, including a PIP, a contract featuring standard data protection clauses, as prescribed by the UDPO, must be executed between the University, through the unit or office concerned, and the service provider. A contract between the University and a PIP shall be referred to as a Data Processing Outsourcing Agreement (DPOA).

In lieu of said clauses, a separate Data Protection Covenant, as prescribed by the UDPO, may also be executed by the parties.

NDAs, standard confidentiality clauses, standard data protection clauses, and DPOAs, as mentioned above in Sections 5.1 and 5.7, will be taken up in greater detail in a separate UDPO Advisory. Samples or templates will also be made available via the UDPO website.

Failure to observe these guidelines may expose the University, through an erring unit or office, to unnecessary risks related to the unauthorized or unlawful processing of personal data. For this reason, each instance of non-compliance shall merit appropriate action from the University, without prejudice to any other liability that a unit or office may incur under all applicable laws.

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

For your guidance.

sgd.

JAMAEL A. JACOB
Director

Noted by:

sgd.

JOSE RAMON T. VILLARIN, SJ
President