The Data Privacy Act of 2012 grants individuals certain rights in relation to their personal data. An organization processing their personal data are obliged to recognize these rights in a manner consistent with the provisions of the law.

This Advisory sets out guidelines for processing requests by individuals to exercise these rights in relation to their personal data under the custody of the University.

May 2019
ADVISORY NO. 19-01

Upholding Data Subject Rights

Background

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), grants individuals certain rights in relation to their personal data. Organizations and other persons processing such data are obliged to recognize and uphold these rights in a manner consistent with the provisions of the law. They must establish and implement mechanisms through which these rights may be exercised.

Within the Ateneo de Manila University, the responsibility for developing these mechanisms lies primarily with the University Data Protection Office (UDPO). Implementation, however, is a duty and function shared by all University offices and personnel. For this reason, the UDPO now issues these guidelines for processing the requests by individuals to exercise their rights in relation to their personal data that are under the control or custody of the University.

1. Scope

This Advisory applies to all offices that process personal data for or on behalf of the University, including their respective personnel, and all personal data under the control or custody of the University. Personal data shall be considered under the control or custody of the University if they are contained in a filing system owned by the University or are meant to be contained in one.

Adherence to this Advisory ensures compliance with the DPA and other applicable issuances of the National Privacy Commission (NPC). Compliance concerns regarding other data protection laws must be referred to the UDPO.

2. Objectives

This Advisory aims to enable the University to uphold the rights of individuals in relation to their personal data, except for the right to be informed and the right to file a complaint, which are covered by a separate UDPO advisory and/or University policy. Specifically, it seeks to:

2.1. ensure that individuals whose personal data are under the control or custody of the University are afforded their rights in relation to their personal data;
2.2. ensure that the University fulfills its obligations both as personal information controller and personal information processor;
2.3. enable the University to demonstrate its commitment to comply with all applicable data protection laws and policies.
3. Definitions

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

3.1. “Approving Authority” refers to any individual or body authorized to decide over a particular issue or transaction for or on behalf of the University.

3.2. “Automated decision-making” refers to an automated data processing operation that serves as the sole basis for making decisions that significantly affect a person whose personal data is processed. There is no human intervention in an automated data processing operation.

3.3. “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.

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

3.5. “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.

3.6. “Data sharing” refers to the sharing, disclosure, or transfer to a third party of personal data under the custody of the University. It excludes the sharing, disclosure, or transfer of personal data to a service provider, or in relation to an outsourcing or subcontracting arrangement.

3.7. “Data subject” refers to an individual whose personal data is processed.

3.8. “Data subject record” refers to a document where the personal data of a data subject are stored and/or recorded. It may be in a paper-based or electronic format.

3.9. “Filing system” refers to any system that is structured or has a referencing mechanism that allows easy retrieval of information about specific individuals.

3.10. “ICT system” refers to an information and communications system, or any part thereof, that generates, sends, receives, stores, or otherwise processes electronic data messages or electronic documents. It includes a computer system or any other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.

3.11. “Office” refers to the basic component or working unit of the University, which includes offices, centers, institutes, departments, and laboratories.

3.12. “Outsourcing” or “Subcontracting” refers to the disclosure or transfer of personal data by the University to a service provider.

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

3.14. “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 ascertained.
3.15. “Personal Information controller” or “PIC” refers to a person, organization, or body who controls the processing of personal data, including a person or organization who instructs another person or organization to process personal data on its behalf. In this Advisory, the University shall be understood as the PIC.

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

3.17. “Privileged information” refers to any and all forms of data, which the Rules of Court and other pertinent laws consider to be privileged communication.

3.18. “Process owner” refers to the office that owns, administers, and/or manages a data processing system, or is the principal custodian of particular personal data being processed by the University. It excludes service providers of the University and their component units.

3.19. “Processing” refers to any operation performed on personal data including, but not limited to, collection, generation, storage, updating, retrieval, use, consolidation, blocking, or destruction of data.

3.20. “Public authorities” refer to any government entity with law enforcement or regulatory functions, as vested by law or the Philippine Constitution.

3.21. “Recipients” refers to any person, organization, or body with whom the University shares, transfers, or discloses personal data.

3.22. “Sensitive personal information” refers to personal information:

3.17.1. about a person’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
3.17.2. 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;
3.17.3. 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
3.17.4. specifically established by an executive order or an act of Philippine Congress to be kept classified.

3.23. “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.

3.24. “Third party” refers to any person, organization, or body other than the data subject and his or her authorized representative, the University, or the latter’s service providers.

3.25. “University” refers to Ateneo de Manila University, including its offices and personnel.

3.26. “University personnel” refer to individuals who perform functions or deliver services for or on behalf of the University. They include, but are not limited to, administrators, faculty members, employees, and consultants.
4. Rights of a Data Subject

Unless otherwise provided by the DPA, individuals have rights in relation to their personal data. They include:

4.1. Right to Access. A data subject may request for certain information regarding the processing of his or her personal data.

4.2. Right to Object. A data subject can object against or withdraw his or her consent to the processing of his or her personal data.

4.3. Right to Rectification. A data subject can demand that any mistake, error, or inaccuracy in his or her data subject record be corrected, updated, or revised.

4.4. Right to Blocking or Erasure. A data subject can ask for the suspension or blocking of the processing of his or her personal data, or request for the removal or deletion of such data, under certain conditions.

4.5. Right to Data Portability. A data subject has the right to obtain a copy of his or her personal data if it is being stored or otherwise processed by the University in a structured and commonly used electronic format.

Other rights not included here will be governed by other UDPO advisories or University policies.

5. General Provisions

All University offices and personnel shall be guided by the following provisions when responding to or addressing data subjects who choose to exercise any of their rights via a request:

5.1. Requesting Party. The following parties may file a request for the purpose of exercising any of the rights provided in Section 4:

5.1.1. data subject;
5.1.2. authorized representative of the data subject, including, but not limited to, the following:
   a. a parent or legal guardian, in the case of a minor;
   b. other individuals to whom a data subject may lawfully assign his or her rights; or
   c. other individuals authorized by law to act for or on behalf of a data subject.

If third parties seek to exercise any data subject right for their own purpose or benefit, a separate UDPO advisory or University policy shall govern. In the absence of such advisory or policy, the DPA, its Implementing Rules and Regulations (IRR), and other applicable NPC issuances will apply.

5.2. Responsible Office. The data subject or an authorized representative shall direct his or her request to the concerned Process Owner (PO), if known. Such PO shall be primarily
responsible for handling the request. If the request is directed at a different office, the latter shall refer the matter to the appropriate PO or, if not known, to the UDPO.

5.3. **Format of the Request.** A request may be filed via email or in person, provided that the PO is able to verify the authenticity thereof, particularly the identity of the requesting party and his or her submissions. As a minimum, the following information and/or supporting documents must be provided to the PO:

5.3.1. date of request  
5.3.2. name and contact details of the requesting party  
5.3.3. data subject’s relationship or established link to the University  
5.3.4. valid identification document of the data subject and a photocopy thereof. Any of the following may be accepted:
   a. any valid University-issued ID with photo, if applicable;  
   b. any valid government-issued ID with photo; or  
   c. Alien Certification of Registration/Immigrant Certificate of Registration, if applicable.

5.3.5. (where applicable) a valid identification document of the authorized representative and proof of such authorization, including photocopies thereof. Proof of authorization may consist of any of the following:
   a. birth certificate, in the case of parents of a minor data subject;  
   b. a properly executed authorization letter or any similar document duly signed by the data subject; or  
   c. other proof of authority to act for or on behalf of the data subject.

5.3.6. (where applicable) other information and/or supporting documents prescribed by the succeeding Sections.

A request shall only be processed upon receipt of all necessary information and/or supporting documents.

5.4. **General Grounds for Denial.** Where applicable, a request may be denied under any of the following circumstances:

5.4.1. when the personal data involved is being processed only for scientific and statistical research purposes;  
5.4.2. when the personal data involved is being processed in connection to an ongoing investigation of a possible criminal, administrative, or tax liability of the data subject;  
5.4.3. there is insufficient or lack of information and/or supporting documents; or  
5.4.4. other grounds as may be provided by law.

5.5. **Processing a Request.** While each PO is free to establish its own procedure to ensure consistency with its internal protocols, it should, as a minimum, take into account the following features:

5.5.1. All requests must be acknowledged in writing upon receipt. Whenever possible, the requesting party must be informed of the expected period of processing.  
5.5.2. Due diligence shall be observed when verifying the identity of the requesting party and his or her submissions.  
5.5.3. In case of doubt, other University offices should be consulted in addressing a particular request.  
5.5.4. Always notify the requesting party of the outcome of his or her request. Where a request is denied, the legal basis therefor and the available remedies for the requesting party must also be provided.
5.6. **Appeals.** If the requesting party is not satisfied with the PO’s decision and/or action, he or she may send a letter of appeal to the UDPO within fifteen (15) calendar days upon notification of the PO’s decision and/or action. Based on the provisions of this Advisory, the UDPO shall review the same and issue a recommendation to the PO. The requesting party shall be furnished a copy of the recommendation. A requesting party or the concerned PO may elevate the matter to the University President as a last resort.

5.7. **Period for Processing.** All requests must be acted upon within a reasonable period of time. The PO shall inform the requesting party if it requires a substantial amount of time to address his or her request and the reason therefor.

5.8. **Fees Schedule.** As a general rule, requests shall be processed at no cost to the requesting party: *Provided,* that a PO may impose reasonable fees when processing requests for hard copies of a data subject record in order to recover administrative costs.

### 6. Right to Access

A request to access certain information regarding the processing of the personal data of a data subject shall be handled in accordance with the following provisions:

6.1. **Subject of Request.** An access request shall be limited to the following information:

   6.1.1. list of personal data being processed, if not known to the data subject or his or her authorized representative;
   6.1.2. sources of the personal data;
   6.1.3. method by which personal data is processed;
   6.1.4. name and contact details of recipients of the data, if any. This includes service providers and third parties;
   6.1.5. reason for sharing, disclosing, or transferring the data to said recipients;
   6.1.6. date and time when data was modified or accessed;
   6.1.7. name and contact details of the process owner and/or the University.

An access request for other information not included in the foregoing list may be denied.

6.2. **Procedure.** In establishing its procedure for processing this type of request, the PO shall determine the mode/s of access the requesting party is entitled to. If it will allow the requesting party to obtain a document featuring the information requested, it must ensure that such document does not include irrelevant, unrelated, or confidential information. Otherwise, it must redact and/or remove such other information prior to the release of said document.

### 7. Right to Rectification

A request to have the personal data of a data subject corrected, updated, or revised shall be handled in accordance with the following provisions:

7.1. **Ground for Request.** A rectification request may be filed in relation to personal data that can be adequately proven to be inaccurate, outdated, or false. A rectification request shall be denied if the requesting party is unable to establish the basis of such request with adequate proof.

7.2. **Additional Submissions.** On top of the information and documents provided in Section 5.3, the following items shall also be featured or included in a rectification request:

   7.2.1. description of the erroneous personal data
7.2.2. specific reason/s for the request
7.2.3. description of the data processing system or activity involved, if known
7.2.4. description of the concerned PO or third party, if known
7.2.5. substantial evidence of the correct, updated, and/or accurate personal data.

7.3. Procedure. In establishing its procedure for processing this type of request, the PO shall:

7.3.1. exert reasonable efforts to make sure other filing systems of the University that feature the erroneous personal data, if known, are also updated;
7.3.2. review and, if possible or necessary, reverse any decision made based on the erroneous data;
7.3.3. notify the recipients of the erroneous data of the update or changes made, if so specified in the request.

8. Right to Blocking or Erasure

A request to have the personal data of a data subject erased or the processing thereof blocked shall be handled in accordance with the following provisions:

8.1. Grounds for Request. Where applicable, a blocking or erasure request may be filed on any of the following grounds:

8.1.1. personal data is incomplete, outdated, inaccurate or false
8.1.2. personal data was collected or processed unlawfully, or without legal basis
8.1.3. personal data is being used or processed for unauthorized purposes
8.1.4. personal data is no longer necessary for the purpose for which it was collected
8.1.5. data subject has raised a valid objection or has withdrawn his or her consent
8.1.6. when the University has violated the rights of the data subject

8.2. Grounds for Denial. In addition to those provided in Section 5.4 of this Advisory, a blocking or erasure request may also be denied under any of the following grounds:

8.2.1. in the case of Section 8.1.1, there is no substantial evidence that the personal data is incomplete, outdated, inaccurate or false;
8.2.2. the request is based on grounds not found Section 8.1 of this Advisory.

8.3. Additional Submissions. On top of the information and documents provided in Section 5.3, the following items shall also be featured or included in a blocking or erasure request:

8.3.1. description of the personal data involved
8.3.2. specific reason/s for the request
8.3.3. description of the data processing system or activity involved, if known
8.3.4. description of the concerned PO or third party, if known
8.3.5. available proof of basis/ground for the request: Provided, that in the case of Section 8.1.1, it shall consist of substantial evidence of the complete, correct, updated, or accurate personal data

8.4. Procedure. In establishing its procedure for processing this type of request, the PO may provide a mechanism for notifying recipients of the personal data involved.
9. Right to Data Portability

A request by a data subject to obtain a copy of his or her personal data that is being stored or otherwise processed by the University in a structured and commonly used electronic format, shall be governed by the following provisions:

9.1. **Subject of Request.** The exercise of this right shall primarily take into account the right of the data subject to have control over his or her personal data that is being processed based on consent or contract, for a commercial purpose, or through automated means.

9.2. **Procedure.** In establishing its procedure for processing this type of request, the PO shall make sure that any information unrelated to the data subject or his or her request, shall be redacted and/or removed prior to the release of the data.

10. Record of Requests

To the extent possible, each PO shall maintain a record that documents all requests it receives, including relevant details such as, but not limited to, the following:

10.1. total number of requests received;
10.2. for each request:
   10.2.1. requesting party;
   10.2.2. action taken;
   10.2.3. response time;
   10.2.4. questions raised, if any;
   10.2.5. challenges encountered, if any; and
   10.2.6. appeal taken by the requesting party, if applicable.

This record must be kept up-to-date to allow the University to address any related inquiry and to demonstrate its compliance with the DPA, if so required by the NPC or the courts.

11. UDPO Review

All parties to a request may consult or seek the advice of the UDPO regarding any or all related issues at any point during the request process. They must provide the UDPO a reasonable amount of time to address their concerns.

12. Complaints

A data subject who intends to file a complaint in relation to the implementation of this Advisory shall do so before the UDPO: Provided, that the process for managing complaints shall be governed by a separate UDPO advisory or University policy. Should the data subject find the UDPO or the University’s response unsatisfactory or unacceptable, he or she may file a separate complaint with the NPC or the courts.
To the extent possible and at the soonest possible time, University offices are strongly urged to establish or modify their internal protocols in a way that is consistent with the provisions of this Advisory.

Failure to observe these guidelines may result in the University’s failure to comply with relevant provisions of the DPA. It may be subject to fines, penalties, and/or other punitive action imposed by the law.

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

For your guidance.

Sincerely,

Sgd.
JAMAEL A. JACOB
Director

Noted by:

Sgd.
JOSE RAMON T. VILLARIN, S.J.
President