

Privacy Policy, Terms of Agreement, and Non-Disclosure Agreement: A Primer

I. Privacy Policy for University Personnel

1. *What is a privacy policy?*

A Privacy Policy (also known as a Privacy Notice or Privacy Statement) informs a person about the way his or her personal data will be collected and used by an organization, group, or another individual engaged in the processing of personal data. It promotes transparency and accountability on the part of the disclosing party.

2. *How many privacy policies does the University have?*

The Ateneo de Manila University currently has four (4) institution-wide privacy policies directed at its primary constituents, namely: (a) students, including applicants and alumni; (b) personnel; (c) campus guests and visitors; and (d) website visitors.

There is no prescribed number of privacy policies that an organization should have. Within the University, a specific unit or office may even develop its own, provided it is consistent with those of the University's. A separate policy may also be drafted for particular data processing systems.

3. *Where can I find the University's privacy policies?*

You can find all the policies at the University website, specifically at:
<http://www.ateneo.edu/udpo/ADMU-Privacy-Policies>

All units and offices are also encouraged to put copies of the policies in conspicuous places where they may easily be accessed and read. For example, the Privacy Notice for Campus Visitors are posted in practically every entry and exit point of the University.

4. *What is the legal basis for having a privacy policy?*

According to Sections 16(a) and (b) of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), a person has the right to be informed about the way his or her personal data will be collected and used by an organization, group, or another individual engaged in the processing of personal data, save for a few recognized exceptions. To uphold this right, the entity engaged in data processing usually develops a privacy policy. This is consistent with the principle of transparency, and also reflects such data privacy principles as fairness, purpose specification, openness, and accountability.

All data protection laws provide for these legal bases (i.e., right and principles).

5. *Is it mandatory for the University to have a privacy policy?*

In a manner of speaking, YES, because: (a) the DPA recognizes the right of a person to be informed about the processing of his or her personal data; and (b) upholding this right is most effectively done via the use of a privacy policy.

It is important to remember, though, that the law does not specifically say that it has to be written down, printed, or published. It may be relayed in any format deemed most appropriate given the prevailing circumstances.

6. *Is the Ateneo de Manila University the only school with a privacy policy?*

NO. Other schools already complying with the DPA and other applicable data protection laws and policies also have one.

7. *Do I need to give my consent to a privacy policy before it becomes effective?*

NO. A privacy policy is only meant to inform. As in the case of other policies of the University or other organizations, your permission is not necessary before a privacy policy is developed and published.

A few months ago, you will recall receiving e-mails informing you about changes in the privacy policies of various internet or online platforms you are using. You may have noticed that the companies did not ask for your permission or consent before they made changes to their privacy policies. By continuing to use their platforms, you are deemed to have agreed to their policies.

8. *Doesn't the DPA now require the University to ask for my consent each time it wants to collect and/or use my personal data?*

NO, it does not. While consent is a basis for collecting and using a person's personal data, it is just one of several lawful grounds. For instance, if a law is requiring the University to collect your data and then share it with a particular government agency, then the University has to comply with such a directive, even without your consent.

To learn more about these other grounds, you may refer to Sections 12 and 13 of the DPA.

9. *Who determines what will be included in the Privacy Policy?*

While the DPA determines the types of information that should be relayed in a privacy policy, it is ultimately the entity engaged in data processing that determines what information will actually be collected and processed. For example, while the law says that the different uses personal data will be subjected to should be in its policy, it is actually Ateneo that determines how it uses the personal data it collects or generates.

To learn more about the information that ought to be included in a privacy policy, you may refer to Section 16 (a) and (b) of the DPA.

10. *Is the Privacy Policy for University Personnel the only one that applies to me?*

NO. Depending on the circumstances, other privacy policies – current and future – may also apply to you. For instance, you may also be pursuing graduate studies in the University, or you are an

alumni of the University; in which case, the Privacy Policy for Students, including Applicants and Alumni, would also apply to you.

11. *Looking at the Privacy Policy for University Personnel, it seems the University is doing a lot with my personal data. Are all of them legal?*

In the regular course of its operations, the University does a lot of things with your personal data, and it is mostly out of necessity. From choosing among job applicants, to providing basic services, to processing an employee's resignation or retirement, the University needs to process personal data to get things done. It does so in a manner that it considers to be fair and lawful.

If any personnel believes otherwise, he or she can raise this concern with the University Data Protection Office (UDPO), and eventually, the National Privacy Commission (NPC) or the courts.

12. *Does the Privacy Policy for University Personnel contain everything I need to know about the way Ateneo collects and uses my personal data?*

NO. The DPA provides for a list of information that need to be included in a privacy policy. There may be other information not on this list that a person may be interested in. According to Section 16(c) of the DPA, an individual may inquire further about the following details regarding the processing of his or her personal data:

- a. contents of personal data that were processed
- b. sources from which the data were obtained
- c. names and addresses of the recipients of the data, if applicable
- d. manner by which the data were processed
- e. reasons for the disclosure of the data, if applicable
- f. information on automated decision-making processes, if any
- g. date when the personal data were last accessed and modified
- h. designation, name, or identity and address of the entity collecting and using the data

The University can also choose to include in the policy other information it deems necessary, even if this is not explicitly required.

13. *Can I inquire about or clarify the contents of the Privacy Policy? If so, how?*

YES. You may send your inquiries and clarifications to following:

University Data Protection Office
info.udpo@ateneo.edu
426-6001 ext. 4801
Rm 200, Manila Observatory, Ateneo de Manila University, Quezon City

Office of Human Resources Management and Organization Development
hrmod@ateneo.edu
426-6001 ext. 4120 to 4129/4155 to 4159 / 4165 to 4169 / 4216
Rm 201 2/F Faber Hall, Ateneo de Manila University, Quezon City

In some cases, you may be referred to another unit or office of the University which may be better positioned to answer your question.

14. *Can I challenge the Privacy Policy or some parts of it? If so, how?*

YES. You may raise your concern to the UDPO through their contact information.

15. *What can I do if I think the University is violating its own Privacy Policies?*

You may report your concern to the UDPO for appropriate action. If not acted upon, or you are not satisfied with the response of the University, you may bring the matter to the NPC.

II. Terms of Agreement: Processing of Personal Data

1. *What are the Terms of Agreement (ToA)?*

The ToA is a document that will subsequently form part of your main contract with the University. Through it, you allow the University to collect and use your personal data for *specific* purposes, or in a *particular* way, or in *certain* instances, as indicated in the document.

2. *How is the ToA different from a Privacy Policy?*

Both documents lay down lawful grounds for the University's collection and use of your personal data. The main difference is that a Privacy Policy does not need your consent to become effective. Meanwhile, the ToA is just a piece of document if it does not contain your consent, as evidenced by your signature or some other indicator. Briefly, a Privacy Policy aims to inform, while a ToA seeks to obtain consent.

In terms of form, there is no prescribed format for a valid Privacy Policy. Consent, on the other hand, must either be in written, recorded, or electronic format in order to be valid.

3. *How is the ToA different from my employment or engagement contract with the University?*

Both represent an agreement between you and the University. The difference is that a ToA pertains specifically to the processing of your personal data. Eventually, the two will be consolidated into one document. For now, though, since your contract is already in force, the ToA and your main contract will be two separate but complementary documents.

4. *Is the Ateneo de Manila University the only organization requiring its personnel to sign a ToA?*

NO. As in the case of privacy policies, organizations that are already complying with the DPA and other applicable data protection laws and policies should have required their personnel to sign one by now, or should at least be in the process of doing so.

5. *What is the legal basis for having a ToA?*

Under the DPA, there are times when the only available ground to process personal data is the consent of the concerned individuals. These instances are usually determined by the type of personal data or data processing activity that will be involved. In the case of the ToA, the document features *specific* data processing activities the University needs or wants to do, but only after it has obtained the consent of its personnel.

You can learn more about the lawful grounds for data processing by referring to Sections 12 and 13 of the DPA.

6. *Why am I being required to sign the ToA just now?*

The ToA and its provisions should ideally be part of your contract with the University. However, since compliance with the DPA is a fairly new requirement for all organizations in the country, it is only now that specific steps are being taken to meet the same (including the use of consent forms). Developing the document and other related data protection measures also took time and involved a rigorous approval process.

7. *Why is signing the ToA mandatory for all University Personnel?*

The data processing activities featured in the ToA generally applies to all University personnel. They include the disclosure of information to authorized third parties like the University's health insurance providers or accrediting organizations (e.g., PAASCU). Accordingly, the document should also be necessary for everyone. Also, since it will form part of your main contract with the University, it becomes mandatory in the same way that your main contract is a prerequisite to your employment/engagement.

8. *Why won't the University just ask for my consent each time it wants to process my personal data?*

The ToA primarily concerns the personal data you provide, or which the University collects or generates, at the start of your work or engagement.

Through it, you do *not* provide your blanket, all-encompassing consent. This means the University will still ask for your consent on separate and future occasions if it will carry out any processing activity involving your personal data that is not specified in the *ToA*.

9. *How long will the ToA be effective?*

The ToA will remain effective for the duration of your work in or engagement with the University, or until you revoke or withdraw your consent, whichever is sooner.

10. *Can I challenge the ToA or some parts of it? If so, how?*

YES. You may also raise such matters with OHRMOD and/or the UDPO through their contact information.

11. *Can I later revoke my signature or withdraw my consent?*

As a general rule in data protection, you may withdraw your consent at any time. However, since the ToA will form part of your main contract with the University (which is not severable), revoking the same will also amount to your rescinding your contract with the University.

12. *What happens if I violate the terms of the ToA?*

The University will take appropriate action against you.

13. *If another University Personnel violates the ToA:*

a. *What will the University do?*

The University will also take appropriate action against such person.

b. *Can I take action against such person? If so, will the University provide me assistance? If so, what type of assistance?*

It is generally the University that stands to incur damage if a person violates the ToA. However, if you feel that you also suffered an injury or incurred damage as a direct result of that person's action or inaction, you may take action against him or her, following the Disciplinary Action Process facilitated by OHRMOD. Remember, though, that OHRMOD can only handle internal administrative complaints.

c. *Can I take action against the University?*

If you feel that you suffered an injury or damage as a result of the University's failure to safeguard your personal data, you may take action against the University as you deem fit.

d. *Can I take action against both?*

If you believe the attendant circumstances support both actions, you are free to pursue them.

14. *If the University transfers, discloses, or shares my personal data with a third party and something happens to such data, causing me injury or damage:*

a. *What will the University do?*

The University will take appropriate action against such third party for violating the terms of its agreement or contract with the University.

b. *Can I take action against such third party? If yes, will the University provide me assistance? If so, what type of assistance?*

YES, you may file a complaint with the NPC or the courts. However, the University can only take appropriate action against such third party for violating the terms of its agreement or contract with the University.

c. Can I take action against the University?

If you believe that any injury or damage that you suffered or incurred is a result of the University's failure to safeguard your personal data, you may also take action against the University.

d. Can I take action against both?

If you believe the attendant circumstances support both actions, you are free to pursue them.

15. *Can I inquire about or clarify the contents of the ToA? If so, how?*

YES. You may inquire and clarify matters with OHRMOD and/or the UDPO via their contact information.

III. Non-Disclosure Agreement

16. *What is a Non-Disclosure Agreement (NDA)?*

An NDA is a contract entered into by two or more parties for the purpose of preventing the unauthorized disclosure of confidential information. In this case, it is between you and the University vis-à-vis any confidential information that you may access or come across while working for or engaged by the University.

Like the ToA, it will also form part of your contract with the University.

17. *What is the legal basis for the NDA?*

As far as personal data is concerned, Section 20(e) of the DPA requires the University to make sure that all its employees, agents, or representatives hold personal data under strict confidentiality, unless they are intended for public disclosure. The obligation continues even after such persons leave the University.

18. *Why is signing an NDA mandatory for all University Personnel?*

The University is required to comply with Section 20(e) of the DPA. On top of that, it is basically a security measure of the University against the unauthorized disclosure of its confidential information, including personal data under its control or custody, and matters covered by its intellectual property rights, among others.

19. *I've been working for the University for years, why am I only being required to sign an NDA now?*

For most personnel, they are already bound to a confidentiality obligation relative to the University, courtesy of a confidentiality clause found in their existing contracts with the school. As such, this NDA only means to clarify the terms of that clause to avoid confusion or issues in the future.

As far as data privacy is concerned, it is a recent development. This explains why it is only now that the NDA is being required in relation to the DPA.

20. *If there is already a confidentiality clause in my contract with the University, why is that not sufficient?*

For enforcement purposes, the confidentiality clause in your contract may suffice. However, as has been pointed out, it is necessary to clarify matters in order to avoid confusion or issues in the future. For example, the existing confidentiality clause does not define what would be considered as confidential information. Neither does it provide for the effectivity period of the obligation. The NDA does both these things and more.

21. *Do I need to sign an NDA every time I need information from the University or any of its units/offices?*

NO. The NDA covers all processing of confidential information during the course of your work for or engagement with the University. However, it does not guarantee that you are free to access or acquire any information under the control or custody of the University. The University will still exercise discretion in determining whether your access to certain types of information is justified or necessary.

22. *Can I just agree with one or some portions of the NDA?*

NO. The provisions of the NDA are not severable.

23. *Is signing the NDA mandatory?*

YES. The University needs to ensure that all its personnel will keep any or all confidential information they access or come across while with the University, including personal data, are kept confidential in order to be able to fully comply with Section 20(e) of the DPA.

It is important to emphasize that it is also meant to benefit you as part of the University. First, it limits the barriers to your access to information. The NDA will also provide the University with additional legal basis for taking action against an individual who misuses or processes your personal data (under the custody of the University) without proper authorization.

24. *What happens if I violate the terms of the NDA?*

The University will take appropriate action against you.

25. *How long will the NDA last? Will it still apply even after I've left the University?*

The NDA, particularly the obligation to maintain the confidentiality of information, will remain in force even after you leave the University, unless otherwise agreed upon in writing by you and the University. This is also mandated by Section 20(e) of the DPA.

26. *If another University Personnel violates the terms the NDA and I am negatively affected by it:*

- a. *What will the University do?*

The University will take appropriate action against such person for violating the terms of his or her contract with the University.

- b. *Can I take action against such person? If so, will the University provide me assistance? If so, what type of assistance?*

If you feel that you suffered an injury or incurred damage as a direct result of that person's actions, you may take action against him or her, following the Disciplinary Action Process facilitated by OHRMOD. You are also free to pursue other legal remedies outside of the University.

- c. *Can I take action against the University?*

If you believe that any injury or damage that you suffered is a result of the University's failure to safeguard your personal data, you may also take action against the University.

- d. *Can I take action against both?*

If you believe the attendant circumstances support both actions, you are free to pursue them.

IV. Others

1. *Because of the University's Privacy Policies and/or because I signed the ToA, will the University now just give my personal data to anyone?*

NO. The University does not automatically disclose, transfer, or share your personal data to any person, office, or entity, even if such disclosure is indicated in the Privacy Policy or is allowed by the ToA or any other consent form that you may have signed. The University will still assess and evaluate every request or demand for your information in order to ensure that you and your personal data are protected.

2. *If a fellow University personnel collects and/or uses my personal data without my consent, can I invoke any of these policies or documents in filing a complaint against him or her?*

NO. A University personnel's collection or use of your personal data for personal reasons does not fall under the privacy management program of the University, because it neither involves a data processing system of the school, a data processing activity it has authorized, nor personal data under its control or custody.

This does not mean, though, that that person is without any liability. He or she may still be held accountable for violating other applicable University policies, such as the Code of Discipline for University Personnel.

3. *If a student collects and/or uses my personal data without my consent, can I invoke any of these policies or documents in filing a complaint?*

NO. As in the case of University personnel, a student's collection or use of your personal data for personal reasons does not fall under the privacy management program of the University.

But again, this does not mean you are without recourse to any legal remedy. That student may be guilty of violating other University policies such as the Code of Conduct for Students. He or she may be held accountable under that policy.