University of the Philippines Diliman
Data Protection Office

upd.edu.ph/privacy

dpo.updiliman@up.edu.ph

(632) 8255-3561

27 May 2020

MEMORANDUM

Reference No. EBM 20-08

FOR	:	Deans, Directors, Heads of Units, Faculty, REPS, Staff, Information Officers and Privacy Focal Persons
SUBJECT	:	**REVISED Privacy Policy for Researchers and Research Subjects**

UNIVERSITY OF THE PHILIPPINES DILIMAN

REVISED PRIVACY POLICY FOR RESEARCHERS AND RESEARCH SUBJECTS

WHEREAS, on 11 March 2018, the UP Diliman Data Protection Office issued the UP Diliman Privacy Policy for Researchers and Research Subjects.

WHEREAS, although processing of personal information for research purposes is exempted from the prohibitions of the Data Privacy Act of 2012, nuances in privacy regulations require a more detailed approach in respecting privacy rights in the conduct of research;

WHEREAS, ethical issues in research require a calibrated and responsible approach to data gathering and processing.

NOW, THEREFORE, in recognition of the constitutional and inherent rights of people to privacy and to uphold respect for privacy in the conduct of research, this **Revised Privacy Policy for Researchers and Research Subjects** is hereby promulgated.

PART I.
SCOPE

This Policy governs UP Diliman Researchers and Research Subjects whose personal information, sensitive personal information and privileged information ("Personal Data") are processed by the University.

UP Diliman has several researchers who, in the course of their research, collect personal information. Their work and their researches are in line with the mandate of RA 9500 otherwise known as the UP Charter of 2008 which recognizes the role that the "University shall serve as a research university in various fields of expertise and specialization by conducting basic and applied research and development, and promoting research in various colleges and universities, and contributing to the dissemination and application of knowledge."

UP Diliman is a research university and hence we should foster an environment that realizes the maximum potential of Filipino research within the bounds of privacy regulations and ethical standards under the Data Privacy Act of 2012.

Definition of Terms

For the purpose of this document, the following terms are defined, as follows:

1. ***Research*** refers to all activities arising from or related to any form of academic study or investigation conducted by any UP Diliman faculty, student, REPS, staff, and all those who aid or facilitate such endeavor;
2. ***Research Data*** refer to all data gathered and all information processed due to or resulting from any Research;
3. ***Researchers*** refer to all individuals directly or indirectly involved in a Research;
4. ***Research Subjects*** refer to all individuals who knowingly or unknowingly participate or in any way become part of a Research from whom data or information is directly or indirectly gathered, observed or processed. "Research subjects" include "data subjects";
5. ***DPA*** refers to Republic Act no. 10173, otherwise known as the Data Privacy Act of 2012;
6. ***IRR*** refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
7. ***Data Processing System*** 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;
8. ***NPC*** refers to the National Privacy Commission of the Philippines as created by the Data Privacy Act of 2012;
9. ***Personal Data*** refers to personal information, sensitive personal information, and privileged information as defined by the Data Privacy Act of 2012; and
10. ***Privacy Risk*** refers to the potential loss of control over personal information when a threat exploits vulnerability.

PART II.
NON-APPLICABILITY OF DATA PRIVACY ACT TO RESEARCH

The DPA applies to all types of personal information and to any natural and juridical persons including the personal information controllers and processors who, although not found or established in the Philippines, use equipment, system, facilities located in the Philippines.[1] DPA also provide exceptions and exclusions of the coverage of this law such as "personal information processed for journalistic, artistic, literary or research purposes"[2].

The NPC, in their Advisory Opinion states that, "Note, however, that the law (DPA) does not provide for blanket exemption for research. Such exemption is limited to the minimum extent of collection, access, use, disclosure or other processing necessary to achieve the specific purpose, function or activity"[3].Thus, Researchers still have an obligation to implement necessary security measures to protect personal information they possess, uphold the rights of data subjects, and adhere to data privacy principles and other provisions of the DPA[4].

The Data Privacy Act is not applicable to Research if all of the following requisites are present:

1. Only data minimally necessary to achieve the research objectives are gathered and processed;
2. The data gathered shall be held under strict confidentiality and shall be used only for the specifically declared research purpose/s;
3. The data gathered are to be used only for the needs of scientific or statistical research; and
4. "The research should be intended for a public benefit, subject to the requirements of applicable laws, regulations, or ethical standards"[5].

The DPA is not applicable if the processed personal information is used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the research subject. Moreover, the personal information shall be held under strict confidentiality and be used only for the declared purpose.

PART III.
PROTECTION OF RESEARCH DATA

Data Life Cycle

Personal information gathered undergoes a cycle which Researchers must keep track of and protect at every stage. In so doing, Researchers must identify with certainty the duties and responsibilities of the individuals who have current and future access to personal and sensitive personal information.

---

[1] Data Privacy Act of 2012, Section 4.
[2] *Ibid*., Section 4 (d).
[3] NPC Advisory Opinion No. 2019-017: Research and the data privacy act of 2012, Page 2.
[4] *Ibid.,* Page 2.
[5] Implementing Rules and Regulations of the Data Privacy Act, Section 5 (c).

1. Creation and Gathering of data

The Researcher who gathers data from Research Subjects should require consent, necessary extent of collection, information security, and confidentiality.

2. Storage and Transmission of data

The data created or gathered must be physically and or electronically stored secure locations. The Researchers must ensure data protection and data quality preservation, with an active data inventory.

As much as practicable, Researchers should store and transmit data using official UP Diliman data processing systems and follow the Communications and Email Policy found in the Information Security Policy of UP Diliman.[6]

The data collected or gathered may include personal information such that its storage in devices must be encrypted and must meet, at least, the Advanced Encryption Standard with a key size of 256 bits (AES-256).

Researchers shall designate location for the storage of printed documents and kept it in locked filing cabinets or any safe storage to keep it secure especially against unauthorized access.

3. Usage

The application of Research Data, including data gathered from Research Subjects, collected or gathered shall be in accordance with the research objectives which should be clearly and expressly stated to justify the use of Research Data, including data gathered from Research Subjects.

4. Retention of data

The personal data collected shall only be retained as long as necessary for the fulfillment of the declared, specified, and legitimate purposes from its inception. The Researchers are the custodian of the Research Data, including data gathered from Research Subjects. The following must be considered in a created Research Data, including data gathered from Research Subjects, retention plan:

a. Research objectives;
b. Legal and regulatory guidelines;
c. Sponsor requirements;
d. Ethical standards; and
e. University Retention Policy

The data to be retained must be classified and protected in compliance with the UP Diliman Data Classification Policy.

---

[6] https://upd.edu.ph/privacy/, UP Diliman Information Security Policy, Chapter III.

5. **Disposal and Destruction of data**

   The Researchers shall have the Inventory of the Research Data, Appraisal, and creation of Research Data Disposition Schedule.[7]

   The Researchers shall maintain records with knowledge of the "general information about the data flow within the organization, from the time of collection, processing, and retention, including the time limits for disposal or erasure of personal data."[8]

In all stages of the research, Researchers shall comply with UP Diliman Information Security Policy and Records Management Policy in UP Diliman's Privacy Portal.

Data Privacy Principles

Data gathering and processing in Research should adhere to the principles of transparency, legitimate purpose and proportionality. For each stages of the data life cycle, the following principles below should be observed.

1. **Transparency**

   The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller (i.e. Researcher), his or her rights as Research Subject, and how can be exercised to invoke their rights. Any information and communication relating to the processing of personal data should be easily accessible and understandable in clear and simple language.[9]

   Since research is part of the special cases mentioned in the DPA, research subject may or may not be aware of the research purpose, nature and extent but only to the minimum extent of the processing of personal information.[10]

   Privacy Notice shall provide the transparency needed by the Researcher and Research Subject. The notice should be simple, straightforward, direct, affirmative and respectful. Sentences must be short and in active voice so it will be easier to understand. When enumerating several items, bullet points are advised to be used. Each section of the notice should have an informative heading to accurately describe what follows. The notice must include the contact information of the Researcher and UP Diliman Data Protection Officer, Research Subject Rights, and how to exercise those rights.

   Researchers should also consider translations of the privacy notice and explaining it verbally if the target Research Subject speaks a different language.

[7] UP Diliman Records Management Policy, Part IV.
[8] Implementing Rules and Regulations of the Data Privacy Act, Section 26 (c) (3).
[9] *Ibid*., Section 18 (a)
[10] *Ibid*., Section 5.

2. **Legitimate Purpose of the Researcher**

The Researchers must have a legitimate purpose in processing personal information for every research and hence the following tests must be considered[11]:

a. Purpose Test – The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;
b. Necessity Test – The processing of personal information must be necessary for the purposes of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
c. Balancing Test – The fundamental rights and freedoms of data subjects should not be overridden by the legitimate interests of the PICs, considering the likely impact of the processing on the data subjects.

3. **Proportionality**

The processing of Research Data, including data gathered from Research Subjects, shall be adequate, relevant, suitable, necessary, and not excessive in relation to the research objective.

In accordance therewith, this Proportionality Test may be used:

- Examination on whether or not the measure is necessary to meet the objective – that is, less intrusive ways of achieving the same objective.
- Examination on whether or not the measure chosen for the collection of information is effective in achieving the objective – that is, whether or not it is rationally connected to it.
- Balancing of the proportional benefits in collecting information against the harm to the data subject's privacy.[12]

Security Measures

In general, the research is exempted from DPA. However, the DPA does not provide for blanket exemption of research, in general. Researchers have the obligation to implement essential security measures to protect the personal data they process.[13]

The security measures aim to maintain the availability, integrity and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

---

[11] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
[12] R vs. Oakes, S.C.R. 103, Supreme Court of Canada, 1986
[13] Data Privacy Act, Section 20.

1. Organization Security Measures

a) Researchers may attend or request training provided by UP Diliman Data Protection Office.

The Privacy Focal Person of the unit/office, where the Researcher belongs, can initiate trainings and/or seminars relative to their unit/office's data security. This training/seminar will be presented by UP Diliman Data Protection Office assigned Lecturer.

b) By understanding the Data Life Cycle, the Researchers shall identify privacy risks by conducting privacy impact assessment and proposes measures intended to address the risks.[14]

c) Persons under the Research Team who have access to personal information shall be asked to sign a Non-Disclosure Agreement. This agreement shall hold the person responsible even after the project ended.

2. Physical Security Measures

a) To determine the necessary size and/or location of the storage, the format of data to be collected must be known. All records with personal information shall be kept in a secured location or locked filing cabinets.

b) Research Data, including data gathered from Research Subjects, includes personal information where only authorized UP Personnel and Researchers are allowed to access. Authorized personnel vary in every unit in UP Diliman. Other personnel may be granted access only through a request stating the purpose of such access subject to the approval of the Researcher.

c) To monitor the data access of all authorized UP Personnel and Researchers in the data room or facility, there must log book of entries in the storage room indicating the date, time, duration and purpose of each entry.

d) Researchers should protect all printed and electronic personal data at all times. The Laptop and Desktop Computers shall be locked upon leaving the workstation/s. Passwords/Passphrases shall not be written on or exposed to others.

e) Proper retention, disposal and destruction of records must also be provided and followed. This must be based on the UP Diliman Records Management Policy.

[14] NPC Advisory Opinion No. 2017-03

3. Technical Security Measures

The Technical Security Measures provide the techniques used for authentication and protection against theft of sensitive data and information. It helps authenticate the users' login and data such that only verified user applications can read and access data and applications. The following technical security measures will guide researchers to avoid risks and security breaches.

a) Communication of UP students, faculty and staff using UP Mail (@up.edu.ph) or UP Webmail (@upd.edu.ph) for standard encryption

b) Use of Passphrases such as a sentence or a combination of words, instead of word, as passwords.

c) Regular backup of the data on personal information. The more important the data and or the more data change, the more regular the backup should be made.

d) Within two (2) hours from discovery of the Security Incident or Personal Data Breach, any person – whether or not connected with UP Diliman – should report the incident via email at securityincident@upd.edu.ph and or phone call to both the UP Diliman Data Protection Officer and the Privacy Focal Person having jurisdiction over the unit involved following the Security Incident Management Policy[15].

UP Diliman Data Protection Office provided a guide to protect UP Diliman's information and information systems to ensure their confidentiality, integrity and availability found in Information Security Policy.

PART IV.
ETHICAL PRACTICES IN PROCESSING PERSONAL DATA

Good researchers follow and comply ethical standards and compliance of Research. Failure thereof will increase the privacy risk associated in the processing of personal information. Below are some of the ethical considerations the DPO suggests to be observed[16].

1. *The person collecting must Put himself in the Data Subject's Position*

   Recognize the Data Subject as an Individual and not merely as a consumer: determine the ethical feasibility of your processing by subjecting yourself to the same procedures: would you consent?

[15] https://upd.edu.ph/wp-content/uploads/2019/04/Data-Privacy-Security-Incident-Management-Policy.pdf
[16] NPC Commissioner Liboro's Presentation on Accountability, Compliance and Ethics, April 2019, UP Diliman

2. *Engineer Privacy-conscious Designs*

   Technological and Process design decisions should not dictate our societal interactions and the structure of our communities, but rather should support our values and fundamental rights. Develop and promote engineering techniques and methodologies that fully respect the dignity and rights of the individual.

3. *Be Accountable for What are Collected*

   The principle that personal data should be processed only in ways compatible with the specific purpose(s) for which they were collected is essential to respecting individuals' legitimate expectations.

4. *Think Beyond Consent*

   Individuals are not merely passive objects who require protection of the law against exploitation and not all human behavior can be explained by economic principles which assume human beings are entirely rational and sensitive to economic incentives.

5. *Collect only what Can be Protected*

   Individuals today are increasingly required to disclose much more personal information in order to participate in social, administrative and commercial affairs, with ever more limited scope for opting out. With this, the notion of free and informed consent is placed under enormous strain and it becomes necessary to limit collection to proportionality and legitimate purpose.

6. *Treat Personal Information as extension of Physical Individual*

   The phrase "Once taken, it can never be returned" comes to mind when it comes to assessing risks and opportunity costs. The dignity of the human person is not only a fundamental right in itself but also is a foundation for subsequent freedoms and rights, including the rights to privacy and to the protection of personal data. Privacy is an integral part of human dignity, and the right to data protection was originally conceived to compensate for the potential erosion of privacy and dignity through large scale personal data processing.

7. *Acknowledge Ownership of Personal Data*

   Absolute control over personal data is difficult to guarantee as there will be other concerns such as public interest and the rights and freedoms of others. Control is necessary but not alone sufficient since customers or data subjects are often not fairly compensated for the data they trade.

8. *Safeguarding Human Dignity as Priority*

   It is necessary to ensure that personally-identifiable information, inclusive of big data, can be easily depersonalized to make it harder or impossible to single out an individual: it is important to evaluate accordingly to the wider societal norms and ethics committees when deciding on a large scope.

9. *Prioritize Pro-Consumer Processing*

   The Data Privacy Act mandates that in interpreting the law, any and all policies or procedures must take into account the rights of the Data Subjects—the very same rights held by those who are processing their information. It becomes necessary to remember the purpose of holding, collecting, and processing of the personal information.

10. *Evaluate the Purpose for Collection*

    Even with legitimate purpose, it is vital to check and update current processes as to whether the need to collect has become obsolete.

PART V.
GUIDELINES IN DATA GATHERING AND PROCESSING

The following are guidelines in gathering and processing data:

1. Unless necessary to accomplish the research objectives, do not collect demographics and personal information from respondents and research subjects such as names, age, contact information, sex, health information, educational information, and other information personal to the individual.

2. Do not use or process gathered data other than the legitimate purposes of the research expressly communicated to the research subject.

   In some cases, the research necessitates that the research subject is not fully aware of the purpose of the observation made to him or her. For example, the research is about subconscious bias and hence the research subject cannot be made aware that his/her subconscious behavior is being observed (otherwise, the research subject will make conscious adjustments). In these cases, the researcher must debrief or fully disclose to the research subject the nature, purpose, and extent of the observation and data gathering as soon as there is no more research need to keep the research subject uninformed. If after being informed, the research subject objects to the debriefed purpose of the research or the intended processing of data, then the research must observe the research subject's *right to object* to the processing and *right to erasure* of gathered data.

3. Unless the prior express recorded informed consent of the research subject is obtained, do not reuse or recycle data for other research, even if related to or

arising from the original research initiative. Gathered data should only be processed in accordance with the number of research projects the research subject was made aware of.

4. Research results and output should only contain anonymized or aggregated data. Identities of respondents and research subjects should not be disclosed unless the prior express recorded informed consent of the research subject was obtained.

5. Unless part of the legitimate purpose of the research, there should be no profiling, judgment, or discrimination of the research subject in any manner. This includes psychological, behavioral, medical, physical, financial, racial, sexual, political, social, or any form of profiling, judgment, or discrimination of the research subject.

6. Researchers should keep in mind that research subjects are data subjects whose data must be protected from unauthorized or unnecessary gathering or processing. In case of doubt, data gathering and processing should be to the *minimum* extent necessary to fulfill the legitimate purpose of the research objective with the least intrusion to the privacy of the research subject.

7. Researchers must be aware of and adhere to applicable ethical standards for research.

PART VI.
ACCESS TO RAW DATA

Research Data, including data gathered from Research Subjects, includes personal information. Only authorized UP Personnel and Researches are allowed to access such information. Authorized personnel may differ in every unit in UP Diliman. Other personnel may be granted access by filing a request with the purpose of the access, but subject to the approval of the Research Creator.

Contractors, Consultants and Service Provides can access the Research Data, including data gathered from Research Subjects, but shall be governed by strict procedures contained in formal contracts, which provisions must comply with the Data Privacy Act of 2012, its IRR, and all applicable issuances by the NPC and UP Diliman. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance.[17]

Authorized users of personal information found in the Research Data, including data gathered from Research Subjects, shall abide with the UP System Policy on Acceptable Use of information assets found in https://upd.edu.ph/aup/.

[17] NPC Circular 16-01 Security of Personal Data in Government Agencies, Section 16.

For authorized users who access the personal information online, it shall have an authentication of their identity via a secure encrypted link and must use multi-factor authentication.

Raw Research data, including data gathered from Research Subjects, can be shared if it is anonymized or aggregated.

Any information is considered anonymized if there is no possible means to identify the research subject, that is, the PIC and/or any other persona are incapable of singling out an individual in a data set, from connecting two records within a data set (or between two separate data sets) and from any information in such dataset.[18]

It should be noted that shared anonymized data can never be used directly or indirectly to identify a person.

Raw data may not be reused for other researches unless the research subject provided consent for the reuse of such data.

Raw Research Dataset includes data gathered from Research Subjects and personal information of Research Subjects. The processing will not be exempted from DPA and its IRR. Thus, consent from Research Subject is required before processing of said information.

No identity of any individual may be disclosed in any research work or output unless the prior consent of such individual was obtained.

It should be stated in the Privacy Notice, using clear and plain language, the Research Objective and how will the personal information of the Research Subject be processed. Any disclosure or sharing of personal information must be stated and clearly understandable to the Research Subject.

Accuracy and up-to-date Research Data

Researchers should make sure that personal data are, based on DPA of 2012, "accurate, relevant, and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date"[19] because any inaccuracy or incomplete data may result to incorrect decision and interpretation of the data acquired.

The DPA of 2012 further states that "inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted."[20]

We also note that when updating contact information, careful attention is needed to avoid risks of sending personal information and/or sensitive personal information to unintended recipient/s.

PART VI.

[18] NPC Advisory Opinion No. 2018-068, Processing of Anonymized Personal Data by Electronic Medical Records Provider.
[19] DPA, Section 11 (c).
[20] *Ibid.*

INTELLECTUAL PROPERTIES

In general, copyrights to intellectual property remain with their creator, except in the case of institutional or collaborative work, because the University is expected to generate copyrightable ideas and creative work. Patents for inventions, on the other hand, are generally presumed to belong to the University when these inventions are created with substantial use of University resources.[21]

In the case of a work-commissioned by a person other than an employer of the author and who pays for it and the work is made in pursuance of the commission, the person who so commissioned the work shall have ownership of work, but the copyright thereto shall remain with the creator, unless there is a written stipulation to the contrary.[22]

Personal information obtained from the research are owned by the Research Subjects. Moreover, said information shall not be processed other than the purpose stated on the research.

PART VII.
RIGHTS OF RESEARCH SUBJECTS

As data subjects, research have the following rights that must be observed by researchers:

1. **Right to be Informed**

   This should answer the questions like, "Why you collect and what will you do to my personal data?", "How will you process my personal data?", "Who can I contact for questions?", "How will you protect my personal data?", and "How can I exercise my rights?"

   The Research Subject's personal data should be treated as their personal property. In the same way that the use of any sort of property must be done with an owner's consent, personal data should never be collected, processed and stored by the researcher without the individual's explicit consent, unless otherwise provided by law.[23]

2. **Right to Object**

   Since the processing of personal information is based on consent, the Research Subject can exercise the right to object. When a Research Subject objects or withholds consent, UP Diliman may not be able to conduct academic, administrative and other functions or services related to the Data Subject. The Researcher should stop processing the personal data as they receive objection unless it is needed pursuant to

[21] UP Research Guidebook version 1.2, March 2016.
[22] Intellectual Property Code of the Philippines R.A. No. 8293, Chapter VI, Sec. 178.4.
[23] Data Privacy Protection and Research Involving Human Participants: A Primer (Draft) by Peter Sy, J.C. Navera, Katrina Tan, Fatima Nicolas

a subpoena, for an obvious purposes (i.e., employer-employee relationship), or it is a result of a legal obligation.[24]

3. Right to Access

Research Subjects have the right to demand reasonable access to their personal information. It should be given in a clear and understandable format.

4. Right to Rectification

Research Data, including data gathered from Research Subjects, should be accurate and up-to-date. The Research Subject have a right to dispute the inaccuracy or error in their personal information and demand that it shall be corrected immediately.

5. Right to Erasure or Blocking

These rights of erasure and blocking do not apply to Personal Data, documents, records and accounts which are part of UP Diliman's public records as an instrumentality of the government or as the national university. It may be exercised if there is a substantial proof that the processing of Personal Data is unlawful.[25]

6. Right to Damages

The Research Subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of Personal Data, taking into account any violation of his or her rights and freedoms as Research Subject.

7. Right to File a Complaint

The Research Subject have a right to complain when they see that there is a violation of his or her rights as Research Subject and for any injury suffered as a result of the processing of his or her Personal Data. The Research Subject shall be subject to review by the UP Diliman Data Protection Office when there is a complaint filed by the Research Subject.

8. Right to Data Portability

Where his or her Personal Data is processed by electronic means and in a structured and commonly used format, the Research Subject shall have the right to obtain from UP Diliman a copy of such data in an electronic or structured format that is commonly used and allows for further use by the Research Subject.[26]

---

[24] Implementing Rules and Regulations of the Data Privacy Act, Section 34.
[25] UP Diliman Data Subject Rights and Responsibilities
[26] *Ibid*.

This REVISED Privacy Policy for Researchers and Research Subjects is issued and promulgated this 27th day of May 2020.

(Sgd.) Elson Manahan
Data Protection Officer
University of the Philippines Diliman