

UP Diliman Data Privacy Notes

1

Data - Privacy - Act

Privacy

Right to be let alone

Data Privacy

Right to keep personal information private

Data Privacy Act

Protects persons against unauthorized and unnecessary processing of personal information

2

Data Privacy Act

Protects persons against **unauthorized** and unnecessary processing of personal information

Unauthorized processing of personal information

No informed consent to processing through transparency

3

Data Privacy Act

Protects persons against unauthorized and **unnecessary** processing of personal information

Unnecessary processing of personal information

No legitimate purpose to processing
Amount of processing is not proportionate to specified purpose

4

Data Privacy Act

Protects persons against unauthorized and unnecessary processing of **personal information**

5

Personal Information



Personal Information

Can be used singly or collectively to reasonably ascertain the identity of an individual

Sensitive Personal Information

Subset of Personal Information

May be used to damage or discriminate against a person

Privileged Information

Information intended only for specified recipients

6

Data Privacy Act of 2012

Section 3 (g). **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 the information, or when put together with other information would directly and certainly identify an individual.



7

Data Privacy Act of 2012

Section 3 (l). **Classified information** refers to personal information:

- (1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- (2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- (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
- (4) Specifically established by an executive order or an act of Congress to be kept classified.



8

Data Privacy Act of 2012

Section 3 (k). refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.



9

Data Privacy Act

Protects persons against unauthorized and unnecessary **processing** of personal information

10

Processing

Personal Information

May be processed if there is (1) prior or immediate consent; or (2) lawful necessity

Sensitive Personal Information

May not be processed except if there is (1) prior consent; or (2) non-commercial lawful necessity

Privileged Information

May not be processed except if there is (1) prior consent of all parties; or (2) lawful necessity

13

Data Privacy Act of 2012

Section 3 (j). refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or deletion of data.



14

SEC. 12.

(d) Necessary to protect vitally important interests of the data subject, including life and health;

(e) Necessary in order to respond to comply with the requirements of public order and safety or to fulfill functions of public authority; or

(f) Necessary for the purposes of the legitimate interests of PIC to whom data is disclosed, except where such interests are overridden by fundamental rights of the data subject.

SEC. 13.

– The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing;

(b) Processing of TETO-12yr(p)-3((i)-3(n)7o2 188.77 Tio2 188.7

SEC. 13.


– The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(d) Necessary to achieve the lawful and noncommercial objectives of public organizations: Provided information are not transferred to third parties and the consent of the data subject was obtained;

(e) Necessary for purposes of medical treatment and is carried out by a medical practitioner; or

(f) Necessary for the protection of lawful rights in court proceedings, or exercise of legal claims, or when provided to government or public authority.

19



Freely Given	<i>Not coerced</i>
Specific	<i>Not a broad consent</i>
Informed	<i>Clear and simple terms</i>
Indication of will	<i>Positive act</i>
Evidenced	<i>Written, electronic or other means</i>

20

Rights of Data Subjects

Section 3 (j). refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

21

Transparency

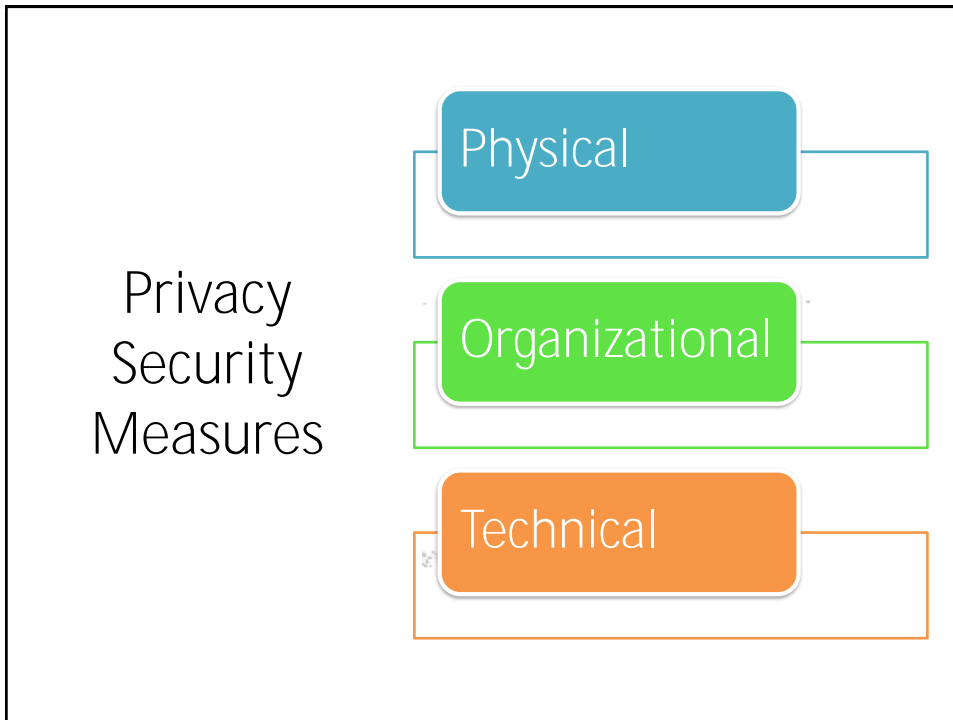
The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data.

Data Privacy
Principles

22

Legitimate Purpose
The processing of
information shall
be

Data Privacy
Principles



25

Jargon

Data Subject

An individual whose personal, sensitive personal, or privileged information is processed

The illustration shows a brown cartoon owl with large eyes and blue-rimmed glasses. The owl is sitting and reading an open book. The book has a brown cover and white pages. The owl is positioned on a surface that appears to be a desk or table, with some colorful, abstract patterns below it.

26

Personal Information
Controller (PIC)

Controls or instructs
the collection,
holding, processing
or use of personal
information



Personal Information
Processor (PIP)

Sub-contractor or
outsourcee

SEC. 30.

Sensitive

-having knowledge of a security breach and of the obligation to notify the Commission but intentionally or by omission conceals the fact of such security breach.

-imprisonment: 1 and 6 months - 5 years +
fine: P500,000.00 - P1,000,000.00

31

SEC. 36.

an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.

32

FINAL REMINDER:

Personal information must, be:

- (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
- (b) Processed fairly and lawfully;
- (c) Accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- (d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

33

Personal information must, be:

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided*, That personal information collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further*, That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing.

34

The UP Diliman Data Protection Office

35

Data Protection Office

Responsibilities of the Data Protection Team

1. Comply with NPC requirements
2. Support services to units of the University
3. Prevent legal, financial, and operational risks
4. Develop in the University a culture of respect for privacy

36

UP Diliman Privacy Portal

upd.edu.ph/privacy

37

UP Diliman Privacy Focal Persons

38

Privacy Focal Persons

Your unit's compliance officer for privacy

UP Diliman has 73 PFPs

Do not hesitate to reach out to your PFP

DPO's projects will be coordinated through PFPs

39

Privacy Focal Persons

Please cooperate with your PFP's Privacy Impact Assessment of your unit or office

40

UP Diliman Policies on Data Privacy

41

Twin Policies on Privacy

Office of the Chancellor Memo No.
MLT 19-061

42

Twin Policies on Privacy

Respecting data privacy

UPD and its people should:

Recognize privacy of students, faculty, staff,
etc.

Identify our to one another

UP Diliman Data Subject Rights and
Responsibilities

Respecting data privacy

For UPD to protect and balance privacy rights:

UPD should also define its own and

UP Diliman Privacy Policy

Twin Privacy Polices

UP Diliman Data Subject Rights and Responsibilities

UP Diliman Privacy Policy

Establish a framework to protect and balance the rights and responsibilities of UP Diliman and its people.

47

Objective

Establish the framework for the interplay of
and between UP
Diliman and its people

48

Data Subject Rights and Responsibilities

49

UP Diliman Data Subject Rights – *OC Memo MLT 19-061*

Right to be
informed

Right to rectify

Right to object

Right to erasure or
blocking

Right to access

Right to damages

50

UP Diliman Data Subject
Responsibilities –
OC Memo MLT 19-061

Respect rights of others

Report breaches

Provide accurate information

Keep information confidential

51

UP Diliman
Privacy Policy

52

Privacy Policy

1. Students, parents and guardians;
2. Faculty (including visiting faculty);
3. Staff (including REPS, UP contractual, Non-UP contractual personnel and retirees);
4. Applicant students, faculty and staff;
5. Researchers and research subjects;
6. Patients, clients and customers;
7. Alumni, donors and donees;
8. Contract counterparties, partners, subcontractors, licensors, licensees; and
9. Other persons related to UP Diliman.

Privacy Policy

are covered by this Policy?

are Personal Data processed?

Personal Data are processed?

UPD Message and Communication Policy

Office of the Chancellor Memorandum No.
MLT-18-135

55

This message, its thread, and any attachments are privileged and confidential. No part of this message may be reproduced or exhibited in any form or manner without the consent of the sender and the University of the Philippines Diliman. In case of wrongful receipt of or unauthorized access to this message, please immediately inform the sender and permanently delete all wrongfully received copies. Your access to this message subjects you to the UP Diliman Message and Communication Policy and relevant data privacy regulations.

56

Clarifications – *OC Memo MLT 18-135*

A Privacy and Confidentiality Notice is required only when all of the following requisites are present:

1. The message is an *"official"* UP message
2. The message contains *"confidential, privileged or personal information"*
3. The message is from the *"University of the Philippines System, including the University of the Philippines Diliman"* and sent to a non-UP external party

57

Clarifications – *OC Memo MLT 18-135*

A Notice is only required for a limited set of instances

There is no mandatory wording for the Notice

Notices are only for non-UP external parties

Not only as email footers but for printed official communications as well

58

Clarifications – *OC Memo MLT 18-135*

Notices are only for non-UP external parties

A Notice is only required for official messages from a UP unit to a non-UP external party (*e.g. from UP Diliman HRDO to the Department of Labor and Employment*).

The UPD Message and Communication Policy states that its Scope are messages "*related to the University of the Philippines System, including the University of the Philippines Diliman, and their respective units*". This does not include internal or personal messages from one UP faculty/staff to another.

61

Non-Disclosure Agreement – *OC Memo MLT-190*

The UP Diliman DPO is open to assist and provide guidance on the NDA.

The UP Diliman DPO's opinions are not necessarily binding because the requirement of signing an NDA was neither an initiative nor a project of the UP Diliman DPO.

62

Non-Disclosure Agreement –
OC Memo MLT-190

There is no mandated format or version of the NDA.

UP Diliman units and offices may draft and word their own NDAs as they may deem proper.