

MEMORANDUM CIRCULARNo. 11
Series of 2023**SUBJECT: DATA PRIVACY MANUAL**


Pursuant to Republic Act No. 10172, otherwise known as the Data Privacy Act of 2012, the Department hereby adopts the attached DSWD Data Privacy Manual.

The Manual serves as a guide to ensure that all personal data collected by the Offices, Bureaus, Services, and Units follows the principles set out in collecting, storing, processing, and sharing personal data in accordance with the Data Privacy Act of 2012.

This Circular shall take effect immediately upon approval.

Let copies of this Circular be issued to the Central Office and Field Offices for their information and guidance.

Issued at DSWD Central Office in Quezon City, Metro Manila.


REX GATCHALIAN
Secretary
Date: JUN 08 2023**Certified True Copy**
MYRNA H. REYES
OIC-Division Chief
Records and Archives Mgt. Division**13 JUN 2023**

DSWD DATA PRIVACY MANUAL

A Guide for DSWD Offices, Bureaus, Services, and Units

VERSION 2.0 – JUNE 2023

DEPARTMENT OF SOCIAL WELFARE AND DEVELOPMENT

**DSWD Central Office IBP Road, Batasan Pambansa Complex, Constitution Hills,
Quezon City, 1126**

DOCUMENT VERSION HISTORY

DATE	VERSION	DESCRIPTION	AUTHOR
06 December 2018	1.0	DSWD Data Privacy Manual	Asec. Noel M. Macalalad
23 August 2019	1.1	DSWD Data Privacy Manual	Asec. Noel M. Macalalad
	1.2	DSWD Data Privacy Manual	Asec. Noel M. Macalalad
24 June 2020	1.3	DSWD Data Privacy Manual	Asec. Noel M. Macalalad Patricia T Joven
22 September 2020	1.4	DSWD Data Privacy Manual	Asec. Noel M. Macalalad Patricia T Joven
26 January 2021	1.5	DSWD Data Privacy Manual	Asec. Noel M. Macalalad Patricia T Joven
05 June 2022	1.6	DSWD Data Privacy Manual	Asec. Noel M. Macalalad Patricia T Joven
16 December 2022	1.7	DSWD Data Privacy Manual	Asec. Irene B. Dumlao Christian Joseph M. Regunay Ijna Alodia P. Santiago
31 January 2023	1.8	DSWD Data Privacy Manual	Asec. Irene B. Dumlao Christian Joseph M. Regunay Ijna Alodia P. Santiago
31 April 2023	1.9	DSWD Data Privacy Manual	Asec. Irene B. Dumlao Christian Joseph M. Regunay Ijna Alodia P. Santiago
01 June 2023	2.0	DSWD Data Privacy Manual	Asec. Irene B. Dumlao Christian Joseph M. Regunay Ijna Alodia P. Santiago

EXECUTIVE SUMMARY

Republic Act No. 10173, known as the Data Privacy Act of 2012, reinforces and formalizes the rights of an individual to privacy. The law guarantees a fair and lawful process that all government agencies must follow in collecting, storing, using, and processing of personal data or information. The law and its implementing rules and regulations provide a set of rules regarding:

1. When to collect personal data;
2. Where to collect; and
3. How to process and share personal data.

The Data Privacy Act of 2012 outlines the type of violations, as well as the corresponding damage claims, monetary penalties, imprisonment terms, as well as administrative sanctions on violators.

The following are the *key terms*¹ needed in order to understand the scope and the basic premise of the law:

- “*Personal Data*” is any information that helps identify a natural person. The law states that the collection of Personal Data is permitted as long as there is a specific, explicit, and legitimate purpose(s). The law further states that no other processing may be carried out in the captured data other than the stated purpose for the collection and processing.
- “*Sensitive Personal Data*” is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade/union membership, health, or sexual preference. Collection of sensitive personal data is not permissible unless such collection is deemed necessary and lawful under applicable law.
- “*Processing of Personal Data*” refers to any operation or set of operations which are performed upon personal data, whether or not by electronic means, including but not limited to collection, organization, storage, adaptation, disclosure, or erasure. It is legal to process personal data if, and only if:
 1. The individual who owns the personal data has given consent;
 2. The processing is necessary to which the individual is a party;
 3. The processing steps are fully disclosed with the individual;
 4. The processing is necessary for compliance of a legal obligation, and
 5. The processing is necessary due to the public interest or the exercise of official authority.

This manual is written to guide the Department of Social Welfare and Development, its officials, managers, and all of its personnel (Permanent, Contractual, Contract of Service, Job Order) in ensuring that everyone follows the principles set out in collecting, storing, processing, and sharing personal data in line with the Data Privacy Act of 2012.

¹ Official definition given by the National Privacy Commission.

I.	BACKGROUND	6
II.	INTRODUCTION	7
III.	SCOPE OF THE DATA PRIVACY MANUAL	8
IV.	DEFINITION OF TERMS	8
V.	LEGAL BASIS	11
VI.	DSWD DATA PRIVACY ORGANIZATIONAL STRUCTURE	12
VII.	SIGNING AND REPRESENTATION IN DATA SHARING AGREEMENTS	13
	A. DATA PRIVACY IMPLEMENTATION CIRCLE (DPIC)	14
	B. ROLES AND RESPONSIBILITIES OF A DATA PROTECTION OFFICER (DPO)	14
	C. ROLES AND RESPONSIBILITIES OF A COMPLIANCE OFFICER FOR PRIVACY (COP)	15
	D. ROLES AND RESPONSIBILITIES OF THE LEGAL SERVICE	16
VIII.	DATA PROCESSING AND ITS CYCLE	16
	A. COLLECTION	16
	B. STORAGE	17
	C. USE	18
	D. DATA PROCESSING ACTIVITY	18
	E. DATA QUALITY	19
	F. DATA SHARING PROCESS	19
	1. GENERAL DATA SHARING PROCESS	19
	2. DATA SHARING PROCESS FOR ACADEMIC /RESEARCH PURPOSES	22
	3. DATA SHARING DURING A NATIONAL STATE OF EMERGENCY	22
IX.	SECURITY MEASURES	23
	A. PHYSICAL SECURITY MEASURES	23
	B. TECHNICAL SECURITY MEASURES	23
X.	BREACH AND SECURITY INCIDENT MANAGEMENT	24
	A. STEPS IN REPORTING A POSSIBLE DATA PRIVACY BREACH	25
	B. ACTIVATING THE BREACH MANAGEMENT PROTOCOL	25

XI.	BREACH INCIDENT REPORTING	26
A.	FINAL BREACH INVESTIGATION REPORT	27
B.	PENALTY AND DISCIPLINARY ACTION	27
XII.	ALIGNMENT PROCESS FOR EXISTING PPS	28
A.	WHO SHOULD CHAMPION THE ALIGNMENT	29
B.	ALIGNING THE DATA CYCLE WITH THE PRIVACY REQUIREMENTS	29
XIII.	PRIVACY IMPACT ASSESSMENT (PIA)	29
A.	THE FIRST STAGE PIA PROCESS	30
B.	THE SECOND STAGE PIA PROCESS	30
C.	WHO WILL BE RESPONSIBLE IN CONDUCTING THE PIA	30
XIV.	OPERATIONALIZING THE DATA PRIVACY PRINCIPLES	30
1.	OPERATIONALIZATION OF PROPORTIONALITY	30
2.	OPERATIONALIZATION OF TRANSPARENCY	32
3.	OPERATIONALIZATION OF LEGITIMACY OF PURPOSE	34
XV.	GENERAL GUIDE IN DEVELOPING A DATA SHARING AGREEMENT	34
	ANNEXES	35
A.	GENERAL PRIVACY IMPACT ASSESSMENT	36
B.	TEMPLATE FOR DATA SHARING AND NON-DISCLOSURE AGREEMENT	48
C.	TEMPLATE FOR BREACH REPORTING	58
	BREACH INCIDENT REPORT TEMPLATE	59
	MANDATORY BREACH NOTIFICATION TO DATA SUBJECT TEMPLATE	63
	ANNUAL SECURITY INCIDENT REPORT TEMPLATE FOR PIC	64
D.	DSWD DATA CONSENT FORM	65

LIST OF FIGURES

Figure 1:	DSWD's Organizational Structure for Data Privacy	12
Figure 2:	Data Privacy Implementation Circle	14

LIST OF TABLES

Table 1:	Designated Representatives and Signatories	13
Table 2:	Potential Penalties listed in the R.A 10173	28
Table 3:	PIA for Data Sharing Assessment Table	31

Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012² ensures that personal data in information and communications systems in the government and in the private sector are secured and protected.³

The law mandates that any entity or organization that collects and processes personal data must establish a set of policies and operational guidelines to guarantee the data's safety including the privacy of individuals, while within the organization's custody and control. All government agencies are therefore instructed to implement reasonable and appropriate security measures to protect personal data against privacy risks, including unlawful collection, unauthorized access, accidental loss or destruction, misuse, unlawful destruction, alteration, and contamination.

In line with this, government agencies are to produce a Data Privacy Manual, as well as educate and train its personnel on the habitual use of such measures in their daily tasks. The Manual is a guide for ensuring the compliance of the Department of Social Welfare and Development to the Data Privacy Act of 2012, its Implementing Rules and Regulations, and other relevant issuances of the National Privacy Commission (NPC).

The Manual provides detailed instructions on privacy and data protection methods and procedures that all personnel must observe and carry out in handling and dealing with personal information. The Manual is the first step toward the fulfillment and realization of protecting the rights of data subjects.

The Department hopes that in due time, all of its systems will exemplify the "Privacy by Design" that the NPC advocates.

² An Act Protecting Individual Personal Information In Information and Communications Systems In The Government And The Private Sector, Creating For This Purpose A National Privacy Commission, And For Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

³ Section 2, Rule I, Implementing Rules and Regulations (IRR) of Republic Act No. 10173, also known as the "Data Privacy Act of 2012".

This Data Privacy Manual comes from the effort of the Department of Social Welfare and Development (Department) to comply with Republic Act No. 10173 or the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and other relevant policies, including other issuances of the NPC. This is subject to the Departments' review and update based on the experiences and initial results of the ongoing implementation.

This Manual serves as the basis of the Department and its personnel in operationalizing its data protection and security measures and in incorporating data privacy measures in the performance of their duties.

The law requires the Department and its personnel to understand and embrace the core **Data Privacy Principles** of the Data Privacy Act, listed as follows:

1. **Transparency.** The Department must ensure that all data subjects understand the nature, extent of processing and the purpose of data collection. In addition, data subjects must be informed of the Departments' data processing and its implications for their right to privacy. The data should be easy for the data subjects to access, update, and request for its deletion.
2. **Legitimate Purpose.** The Department must ensure that all personal data processing must have a legal basis or a legitimate purpose. In most cases, the primary legal basis is often linked to the Departments' mandate, or at the very least, to the attainment of its vision and goal statements. In compliance with the Data Privacy Act, the Department shall ensure that the data processing aligns with the publicly stated purpose of its programs or projects.
3. **Proportionality.** The personal data that the Department will capture, store, process, and use should be no more than what is needed to attain its program requirements or purpose.

Data sharing must always be calibrated to stated legal purposes. All data elements must be examined to ensure that it is essential in order to achieve the stated legitimate purpose.

This Manual ensures that the data privacy rights of all the Departments' personnel and beneficiaries are respected and valued, by ensuring that all personal data collected are processed based on the Data Privacy Principles of transparency, legitimate purpose, and proportionality.

The objectives of the Manual are as follows:

1. To ensure that all personal data collected from the Departments' recipients, personnel, and individuals are processed based on the general principles of the Data Privacy Act relating to transparency, legitimate purpose, and proportionality; and
2. To ensure security measures are in place to prevent unauthorized processing of information.

This Manual shall apply to all Offices, Bureaus, Services, and Units (OBSUs) of the Department. It shall be strictly followed by all its personnel, regardless of position and employment status, including third-party software developers, contractors, and other service providers that may have direct or indirect access to databases and electronic storage that contains personal data.

This Manual serves as the main manual of the Department and shall be a guide for the Programs and Services, including National Program Management Offices (NPMOs) in crafting their Data Privacy Manuals, if applicable.

This shall apply to the processing of all personal data that the Department stores in its PPS databases. It shall cover all stages of the Data Life Cycle of personal data gathered by the Department's processes.

This Manual uses the following key terms to mean:

1. **Access Control List** refers to a list of specifications that provides: (1) the users or system processes that are granted access to objects, and (2) what operations are allowed on given objects.
2. **Compliance Officer for Privacy⁴ (COP)** refers to an individual(s) who perform some of the functions of a Data Protection Officer (DPO). The COP shall be under the supervision of the DPO.
3. **Database Administrators** refers to an individual(s) responsible for operating, maintaining, and securing the Department's database. The Database Administrator must also ensure that the database is appropriately stored and retrieved.
4. **Dataset** refers to one or more records or information collected and retained by a specific office or program in the Department.
5. **Data Collection Form (DCF)** refers to the form used by the Department to collect data from its beneficiaries and inform them that their personal data may be shared with third parties. This form should contain the following:
 - A section that informs Data Subjects of their privacy rights;
 - Clear notification that the information of the Data Subject may be shared with other parties; and
 - Secure consent from the Data Subject to allow the Department to share their data.

⁴ National Privacy Commission (NPC) Advisory No. 01, series of 2017 [Designation of Data Protection Officers]

6. **Data Life Cycle** refers to all of the stages of data throughout its life from its creation for a study to its distribution and reuse. It is typically broken down into creation, storage, usage, archival, and destruction.
7. **Data Sharing Agreement (DSA)/Memorandum of Agreement (MOA)** refers to a signed agreement between the Department and a third party requesting access to the database of the Department's PPS, or vice versa.
8. **Data Subject** refers to an individual whose personal data is captured, stored, and processed by the Department. The term shall apply to the personal data of its officials, personnel, and beneficiaries.
9. **Data Processing** refers to any operation or any set of procedures performed upon personal information, be it manual or electronic means; this includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
10. **Data Protection** refers to the implementation of appropriate physical and security measures to prevent the unauthorized intentional or accidental process, modification, disclosure, and destruction of data.
11. **Data Protection Policies** refers to a set of guidelines and procedures crafted and implemented designed to comply with data privacy and security principles and provisions of the Data Privacy Act of 2012.
12. **Data Protection Officer (DPO)** refers to the personnel of the Department designated by the Secretary to be accountable for the Department's compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations (IRR), and other relevant policies, including other issuances of the National Privacy Commission (NPC).

A DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have a sufficient understanding of the processing operations being carried out by the Personal Information Controllers (PICs) and Personal Information Processors (PIPs), including the latter's information systems, data security, and/or data protection needs. Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.


13. **Department** refers to the Department of Social Welfare and Development.
14. **Ease of Doing Business** refers to the adoption of simplified requirements and procedures that will reduce red tape and expedite transactions in the Department.
15. **Manual** refers to the Data Privacy Manual of the Department of Social Welfare and Development.
16. **Non-Disclosure Agreement (NDA)** refers to a legally binding contract that establishes a confidential relationship whereby parties signing the agreement agree

that sensitive information they may obtain will not be made available to other persons.

17. **Offices, Bureaus, Services, and Units (OBSUs)** refers to various departments and units under the Central Office and Field Office(s) that performs specific function and services.
18. **Personal Data** refers to all types of personal information, which, directly and indirectly, facilitates the identification of an individual. Personal data may be personal information or sensitive personal information.
19. **Personal Data Breach or Privacy Breach** refers to a violation of security which can result in any of the following:
 - Accidental or unlawful destruction, loss, and alteration of personal information;
 - Unauthorized disclosure of, or illegal access to personal data;
 - Unauthorized transmittal, sharing or storing, and
 - Unauthorized processing of information.
20. **Personal Data Processing** refers to any operation or any set of procedures performed upon personal information, be it manual or electronic means, this includes the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
21. **Personal Information**⁵ 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.
22. **Personal Information Controller (PIC) or Data Controller** refers to a person, or any entity, natural or legal, who controls the processing of personal data, or instructs another to process personal data on his behalf.
23. **Personal Information Processor (PIP) and or Data Processor** refers to any natural or juridical person or any other entity to whom a PIC may outsource or instruct the processing of personal data.
24. **Privacy Notice** refers to a statement on what the Department aims to do with a person's data. It contains the following information: (a) personal data involved, (b) purpose of collection and extent of their processing, and (c) safeguards in place to ensure their protection.

⁵ Sec. 3(L) Implementing Rules and Regulations of RA 10173

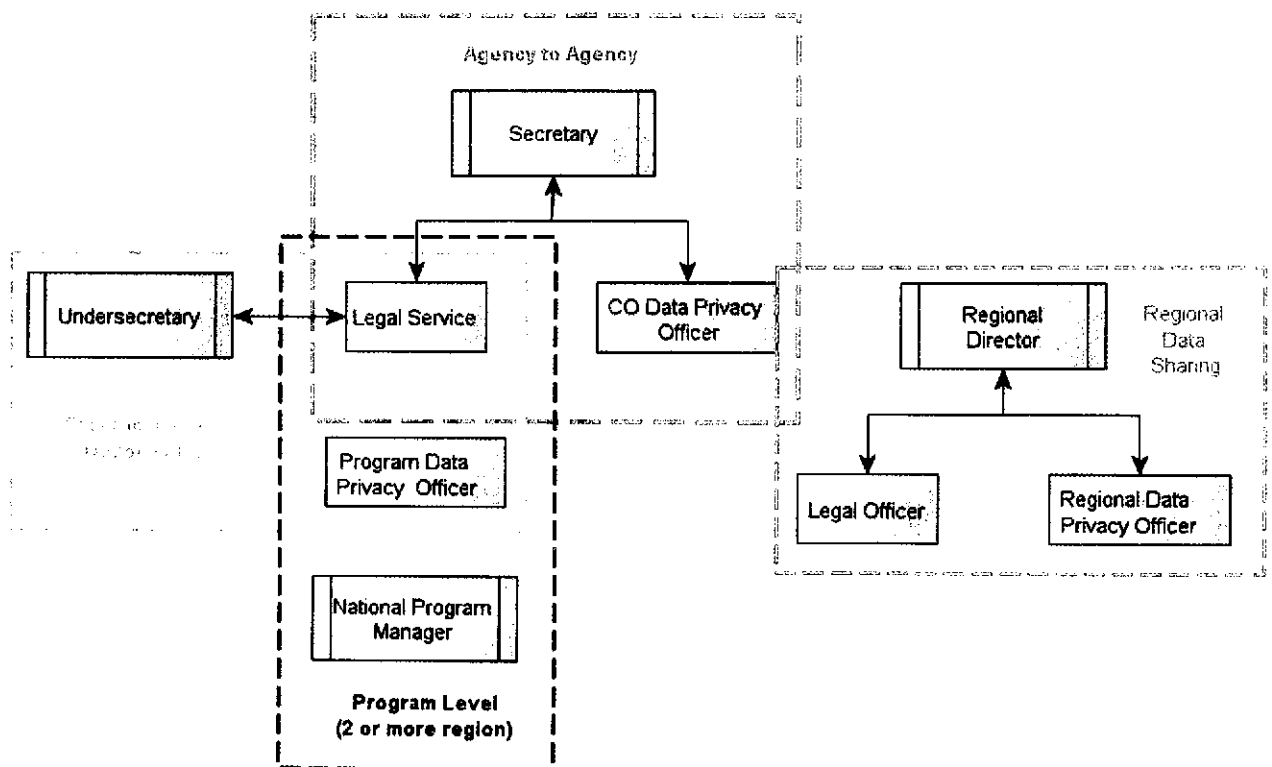
25. **Privacy by Design** is an approach to the development and implementation of projects, programs, services and processes that integrates into the latter's design or structure safeguards that are necessary to protect and promote privacy, such as organizational, technical, and policy measures.
26. **Project, Program and Services (PPS)** refers to social welfare initiatives, interventions, and activities that address the needs of the poor, vulnerable, and marginalized sectors.
27. **Secretary** shall refer to the Secretary of the Department of Social Welfare and Development.
28. **Sensitive Personal Information** refers to types of personal information that often leads to discrimination, marginalization or exclusion of an individual. The following are some of which may be considered as sensitive:
- Data relating to an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - Data about an individual's health, education, the genetic or sexual life of a person;
 - Data relating to any offense committed or alleged to have been committed by such individual, criminal convictions, the disposal of such proceedings;
 - Children's data referring to Personal Information may include name, date of birth, gender, nationality, and civil status;
 - Credit and financial information; and
 - Personal identity numbers issued by government agencies such as social security numbers, previous or current health records, driver's licenses, tax ID numbers, and others.
29. **Privileged Information** refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication.
30. **Third Party(ies)** refers to any individual, organization, contractors, agencies or entity the Department shares with or transfers data.

- 
1. Republic Act (RA) No. 10173 or the Data Privacy Act of 2012
 2. Implementing Rules and Regulations of the Data Privacy Act of 2012
 3. RA No. 6713 or the Code of Conduct and Ethical Standards for Public Officials and Employees

4. Memorandum Circular (MC) No. 8, series of 2020 or the Simplified Data Sharing Guidelines on the Provision of DSWD Programs and Services During a National State of Emergency
5. MC No. 21, series of 2012 or the Enhanced Guidelines on the Code of Conduct for Personnel of the Department of Social Welfare and Development
6. NPC Circular No. 03, series of 2020 or Data Sharing Agreements
7. NPC Advisory No. 01, series of 2017 or Designation of Data Protection Officers
8. NPC Circular No. 02, series of 2016 or Data Sharing Agreements Involving Government Agencies

The Department is one of the largest collectors of personal data of individuals. The Department collects data from its officials, personnel, partners, and beneficiaries, which includes, but is not limited to, personal information about children, men, women, and older persons in need of various Social Welfare Programs and Services. Protecting privacy, therefore, requires equitable distribution of the responsibility among its officials and personnel. The figure below shows the Department's organizational structure for Data Privacy:

Figure 1: DSWD's Organizational Structure for Data Privacy



The Department is a Personal Information Controller (PIC). It assumes ownership and the responsibility of securing the data collected by its PPS, especially those that are private and sensitive.



The Secretary shall represent the Department in entering into a DSA with the third party. However, due to numerous data sharing requests that the Department receives, and in compliance with the requirements of Ease of Doing Business, the Department designates the following representatives for various data sharing mode:

Table 1: Designated Representative(s)

Scope of Data Sharing	Authorized Representative(s)
Data Sharing Agreements involving a region's dataset	Regional Director
National Programs requiring nationwide dataset	Undersecretary in charge of the program
National programs but limited to two or more regions but not nationwide datasets	National Program Manager
National programs covering just one region ⁶	<ul style="list-style-type: none"> ● If partnership is initiated at the region, Regional Director ● If partnership is initiated by a Program Director, Program Director ● If partnership is initiated at the CO, National Program Manager

The National Privacy Commission (NPC) requires all NGAs to appoint a DPO who shall oversee the implementation of their data privacy regulations. However, given the size and number of databases that the Department maintains, the NPC, through its Monitoring Division has agreed to recognize and register several DPOs in the Department.

Thus, the following offices are required to identify and appoint its own DPO:

1. Human Resource Management and Development Service (HRMDS);
2. Information and Communications Technology Management Services (ICTMS);
3. National Household Targeting Office (NHTO);

⁶in case of possible confusion as to signatories and representatives, refer to the table on national programs covering just one region.

4. Project Management Bureau (PMB);
5. Pantawid Familyang Pilipino Program-NPMO (4Ps-NPMO);
6. Sustainable Livelihood Program-NPMO (SLP-NPMO);
7. Kapit-Bisig Laban sa Kahirapan – Comprehensive Integrated Delivery of Social Services- (KALAHI CIDSS)-NPMO; and
8. All Field Offices (FOs).

All other OBSUs shall have the option to designate a Compliance Officer for Privacy (COP).

A. DATA PRIVACY IMPLEMENTATION CIRCLE (DPIC)

The implementation of data privacy is a huge organizational and operational challenge. In response to this need, the DPIC shall be formed to provide the mechanism and platform for discovery, sharing of implementation experiences, and learning across different OBSUs. It shall provide the core mechanism that will assist the Department in updating and enhancing the privacy implementation covering policies, issuances, and other modes for institutionalizing the practice of “Privacy By Design”.

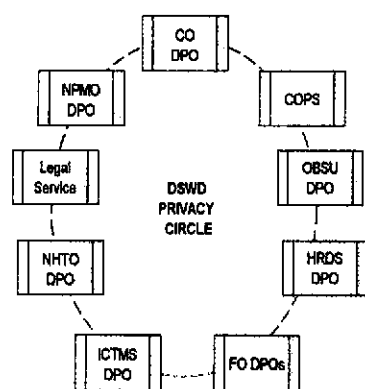


Figure 2: Data Privacy Implementation Circle
The primary role of the DPIC is to develop policies, guidelines and other mechanisms of the Department in the field of data privacy and data protection in order to fully operationalize “Privacy by Design.”

The DPIC shall be composed of privacy practitioners coming from various offices that process databases. It will also include all those offices that work with and process personal data of people. Initially, it will be composed of all DPOs, COPs, the Legal Service and DPOs of national programs.

B. ROLES AND RESPONSIBILITIES OF A DATA PROTECTION OFFICER (DPO)

DPOs shall lead the development of Data Protection Policies (DPPs), and set and align the Departments' workflow and process standards with the requirements of the Data Privacy Law.

The DPOs shall be responsible for the following:

- Educating the Department and its personnel regarding compliance requirements;

- Training personnel in proper ways of data processing;
- Conducting audits to ensure compliance;
- Proactively address potential issues;
- Being the point of contact between the Department and NPC;
- Monitoring the Department's performance in the implementation of its DPPs;
- Maintaining a registry containing records of all data processing activities, the purpose of all processing activities, all access to databases;
- Interfacing and informing the data subjects where the Department uses their data; and
- Informing the data subjects of their rights, and the measures that the Department uses to protect their personal data.

C. ROLES AND RESPONSIBILITIES OF A COMPLIANCE OFFICER FOR PRIVACY (COP)

The COPs shall be responsible for the following:

- Ensuring that all office procedures conform to the privacy protocols. All other OBSUs such as Human Resource Bureau, which collect Personal Information of the Department's personnel, as well as, the Standards Bureau which collects registration information of Social Work Agencies (SWA's), Private Organizations (PO's), and others in both Central Office (CO) and FOs and others that manages personal information other than beneficiaries or individual shall also elect a COP;
- Ensuring that daily activities of the PPS, especially activities that process personal data, follows the prescribed privacy protection procedures;
- Ensuring that the OBSU is conducting its operation and personal data processing in full compliance with this Manual;
- Assisting in the education of all the personnel in their respective offices, as well as the beneficiaries and other Data Subjects on the merits of the privacy law and how the Department is complying with the requirements of the law, and
- Assisting in the review and identification of gaps in the policies and operating procedures.

D. ROLES AND RESPONSIBILITIES OF THE LEGAL SERVICE

The Legal Service (LS), as the legal arm of the DSWD, shall ensure that all agreements entered into by the Department with the Third Party are within the bounds of the Data Privacy Act. It shall also provide legal opinion on various data privacy matters that may arise between the OBSUs and a third party. This role ascertains that the data sharing requests are thoroughly reviewed and in accordance with the Data Privacy Act, its future amendments, and other related issuances.

In case of a data breach, the Appointed DPO shall immediately create an AD HOC Team composed of the office where the breach incident happened. The LS, the Appointed DPO, other offices, officials, or personnel may be included as necessary.

Data Processing refers to the act of collecting, storing, sharing, manipulating, and/or translating data into usable information. The output of a data processing activity is referred to as "information" or sometimes called processed data. This information is formatted and disseminated as reports. Personal information and sensitive personal information of a person collected by any OBSUs are processed using the same data processing cycle.

The Department collects, processes, uses, and shares personal data guided by applicable laws anchored and balanced on what is deemed reasonable, practical and appropriate based on the stated PPS goals or objectives.

The Department recognizes that the collection of personal data requires the consent of the data subject. The Department also recognizes that consent from the data subject should be unambiguous, explicit, and subject to cancellation any time by the individual or the data owner.

In order to prevent unlawful, unauthorized disclosure, alteration, and any other prohibited forms of data processing, all OBSUs collecting personal data shall have their own data collection form indicating the specific purpose of collection. All OBSUs shall also establish and implement suitable technical and organizational measures in implementing the Data Life Cycle.

The collection, storage, use, and sharing of personal data are only valid under the following circumstances:

A. COLLECTION

The Department, in leading the provision of social protection, collects personal information and personal sensitive information of its personnel and beneficiaries.

These data may be stored in database(s) that will allow the Department to study and design appropriate programs, projects, and services, including the use of the data for developing policies and other related instruments. In such cases, the Department shall adhere to the requirements of the Data Privacy Act, its IRR, NPC issuances, and other relevant policies.

The collection of data from beneficiaries shall require the use of a **Data Collection Form (DCF)**. All DCFs shall feature a Privacy Notice which shall contain the following:

1. The purpose of the data collection;
2. Data subjects' right to privacy;
3. The right to refuse collection and sharing of personal information;
4. The right to complain and where to complain when their privacy is breached;
and
5. Period of retention.

The form shall notify and request the data subject to allow the Department to collect and share their personal data. Personal data collected in this manner enables the Department to readily collaborate with Social Welfare and Development partners, other NGAs, and LGUs, subject only to conditions of the approved and signed DSA such as:

1. Data subject to whom the personal data relates shall give its consent to capture his or her personal data;
2. Collection of personal data, especially all sensitive personal information, shall be carried out in line with the Department's legal mandate, vision, thrusts, and priorities; and
3. PIC and relevant DPO shall approve the collection processes and forms before actual use.

Failure to obtain the consent of the existing beneficiaries, the Department shall delete the personal data collected *unless* there is a legal basis or legitimate reason for retaining the data. Consent of data subjects is necessary in every step of data processing cycle which includes collecting, storing, sharing, manipulating and/or translating data.

B. STORAGE

All personal data in the Departments' database(s) shall remain until the approved retention period. The length of time for storage is dependent on the stated purpose of collecting the personal data, including any applicable legal storing periods as prescribed by the National Archives and other oversight agencies.

The Department shall delete all personal data permanently and securely after the retention period. All PPS shall include a data retention schedule as an essential part of proposal paper. The proposal shall state the nature and kind of data needed, purpose of its collection and processing, periodic update of databases, and retention period. Upon approval, the retention period set shall serve as the basis for storage alongside prescription from other oversight agencies.

If the retention period needs to be extended, renewal of the DSC indicating the changes made in the holding or retention period must be entered into by both parties.

C. USE

The use of personal data shall only be allowed when it is necessary to the PPS goals and objectives. Use of personal data may also be allowed if:

1. For compliance with a legal obligation to which the Department is mandated;
2. To protect the vital interests (welfare and development related concern) of an individual;
3. For the performance of a task carried out in the public interest or the exercise of the Department's official function;
4. For purposes of a legitimate interest pursued and approved PPS by the Department's EXECOM and MANCOM, and
5. In compliance with other laws and regulations and other legal purposes.

D. DATA PROCESSING ACTIVITY

Processing of personal data shall only be allowed when it is essential to the attainment of the PPS goals and objectives. There are two ways by which personal data may be processed: (i) internally or (ii) via data processor. In both instances, data processing shall only be allowed under the following circumstances:

1. The Department's officials and personnel, or a data processor **and other contractors** who have access to personal data must only process the data guided by the pre-stated purpose of the processing, and should not share, distribute, or otherwise disclose the personal data to anyone unless given specific instruction to do so;
2. During processing, all are enjoined to apply appropriate technical and organizational measures to protect personal data against accidental, unlawful destruction, unexpected loss, alteration, unauthorized disclosure, access, and any other prohibited forms of processing, which includes:
 - unauthorized copying of some or all data in the database;
 - unauthorized alteration and/or deletion in full or in part of the data; and
 - unauthorized printing of some or all data in the database.
3. The extent of such measures should be appropriate to the risks represented by the processing, and nature of, the personal data; and

4. In case the data processing will be outsourced via a data processor, the DSA must be signed between the Department or OBSUs, and the authorized representative of the data processor. In addition, the DSA for outsourced data processing shall include the retention period and agreed process for deletion of the data.

The Department shall allow the sharing of personal data only when the PPS concerns social welfare and development.

E. DATA QUALITY

The processing of personal data shall be necessary to achieve the PPS purpose(s) and objective(s). Processing of personal data shall comply to the following Data Quality parameters:

1. Processing shall be relevant to the purpose(s) for which they are to be used and to the extent necessary for those purpose(s); and
2. Personal data must be correct, accurate, and, to the extent necessary, updated.

F. DATA SHARING PROCESS

The Department has been approached for its databases for several reasons, ranging from PPS development, partnership implementation, research and development, studies and thesis, etc. In response to this, the Department prescribes the following procedure that shall be observed for data sharing:

1. GENERAL DATA SHARING PROCESS

1. Data sharing shall be preceded by a prior privacy notice and disclosure agreement signed by the data subjects whose personal data are involved in the request. In its absence, the Department shall notify and secure the consent of all the data subjects concerned.
2. All existing PPS of the Department, e.g., 4Ps, SLP, KALAHY-CIDSS, etc., shall distribute privacy notice and disclosure agreement forms to its existing beneficiaries. The notices shall, at a minimum, contain the following information:
 - i. The name of the third party;
 - ii. Legitimate or legal purpose(s) for requesting access to the personal data or objective of the processing of the personal data;
 - iii. Provide a list of data to be accessed and the name of DPO in charge and his or her contact information;
 - iv. Any other information necessary for the data subject to exercise their privacy rights; and

- v. Only those who agreed to share their personal data may be shared with the third party.
3. All sharing of data, either in whole or in part, shall be covered by a DSA. (See *Annex A: Sample Template/Memorandum of Agreement/Data Sharing Agreement.*) Here are the prescribe steps to follow prior to signing a DSA:
 - i. All partnership and collaborative PPS design processes shall sign a Memorandum of Understanding (MOU) or a Memorandum of Agreement (MOA). This agreement shall establish the legality the partnership and possible data sharing agreement, and define the common purpose, objectives and directions of the parties.
 - ii. The agreed purpose, objectives and directions shall be examined. Both parties shall determine if data sharing is necessary, and agree that data sharing is the only means by which the PPS' purposes, objectives and directions can be achieved.
 - iii. Exercise of Proportionality. This is the most important step in crafting data sharing agreements as each purpose must be laid down and the objectives with each purpose must clearly be associated. The use of a matrix is recommended to be used in establishing association. In addition, the data needed to attain the objectives must also be determined.
 - iv. Craft the DSA using the data, objective, purpose linkages.
 - v. Determine how long the PPS will retain the data.
 - vi. Agree on the baseline security measures, e.g., conduct inspection.
 - vii. Design and agree on the data transfer process, ensuring security of data while on transit.
 - viii. Identify the authorized personnel to receive and process the data.
 - ix. Formalize the DSA by having it signed by both parties.
4. Transfer and access to the database(s) shall strictly follow the agreed data sharing process stated in the signed DSA. The actual transfer of data shall take place under the following sign-off scenario:
 - i. The Department shall present and discuss the salient features of the Data Privacy Act of 2012. The third party must sign the

acknowledgement that they know the extent of their roles and responsibilities relative to the privacy of the data to be transferred.

- ii. Successful completion of Pre-Inspection Meeting. The Department shall check for the duly registered DPO of the third party. The third party shall submit the name of the DPO through a letter signed by the appropriate authority.
- iii. An Inspection Meeting shall be conducted to check for the presence of the following security measures:
 1. Organizational;
 2. Physical;
 3. Procedural; and
 4. Technological security measures.

The key activities above shall require the sign off certification that attest to the capability of the third party to secure the personal data. This ensures that in case of a breach, the Department and its representatives in the data sharing are legally protected.

The agreement is sealed with a Memorandum of Agreement, Memorandum of Understanding, or any other legal instrument attesting to the partnership or collaboration. At this stage, a copy of the agreement should be submitted to the Appointed DPO, not for comment, but to allow the DPO to review and prepare for a possible Data Sharing Agreement (DSA). It is advisable that the legal document identifies the need to conduct data sharing early, and the general purpose of the data sharing should be stated in the document. General purpose agreements could be "improve the livelihood of the beneficiary," "improve the nourishment of a non-school aged child," or "provide assistance to victims of family violence." This type of statement provides the DPO and other readers with information about the general intent of the partnership.

The partnership should discuss who is the data owner. It is important that this be established early. The data owner is the Privacy Information Controller (PIC) and is the one responsible for ensuring that data is given the required protection as specified in the law all throughout the entire partnership. The data owner or the PIC is the entity that requested the data owner to share his/her personal data and is, therefore the keeper of the data owner's "trust." The entity receiving the data is the Personal Information Processor (PIP).

Once the partnership agreement has been signed, the next thing that must be established is what data must be shared. In order to establish the requirement, it is necessary to review the general purpose of the partnership. Example, if the partnership agreement is about "improving the livelihood." The partnership should

establish the explicit purpose for data sharing or the 5W (who, what, where, when, why) and one H (how) e.g.:

- Improve the income potential of the Household head;
- The program will provide 5 weeks of intensive training via personal choice of TESDA accredited program;
- The program will start from June to August of 2022; and
- etc.

Once all the necessary details of the objective are agreed upon, it is time to operationalize the three data privacy principles, which are: transparency, proportionality and legitimate purpose.

2. DATA SHARING PROCESS FOR ACADEMIC/RESEARCH PURPOSES

The Department receives data sharing requests from the academe and its students for academic and research purposes, private entities for welfare and development purposes, and Non-Government Organizations (NGOs). In response to this, the Department prescribes the following procedure that shall be observed in sharing data:

1. For Academic and Research Purpose (Students)

Sharing of personal data of the Department's beneficiaries is discouraged. However, demographic information and anonymized datasets may be shared.

2. For Business (Private Commercial Entity and/or NGO) purpose

Private entities and NGOs shall provide a legitimate purpose for accessing personal data. It is necessary that the data sharing process presented above shall be followed, most especially if the data sharing involves sensitive personal information.

3. DATA SHARING DURING A NATIONAL STATE OF EMERGENCY

In cases where the Philippines is declared under a state of National Emergency, and other NGAs, LGUs, or other organizations are requesting for the Department's database of a PPS, the concerned OBSU may refer to Memorandum Circular No. 8, series of 2020 or the Simplified Data Sharing Guidelines on the Provision of DSWD Programs and Services During a National State of Emergency.

[REDACTED]

Data security is the practice of protecting information from unauthorized access, corruption, or theft throughout its entire lifecycle. It is a concept that encompasses every aspect of information security from the physical security to administrative and access controls, and logical security of software applications. It starts with the development of organizational policies and procedures pertaining to data security.

A. PHYSICAL SECURITY MEASURES

The Department maintains a hybrid mix of electronic and physical records that contains personal data. The following physical security measures shall be implemented:

1. All records (analog and digital) containing personal data shall be kept in a secure location in the office. It shall follow relevant regulatory prescriptions set out by the National Archives, Department of Information and Communications Technology (DICT), Commission on Audit (COA), Department of Budget and Management (DBM), and other government oversight agencies that provide guidelines and specifications on records management and storage (digital or analog);
2. All digital records shall be in a secure data center compliant to the standards that may be prescribed by the DICT;
3. Secured data center must have a secured access area where only authorized personnel are allowed to enter;
4. Secured data centers shall maintain a list of Database Administrators who will have administrative access to the databases;
5. All database administrators must sign a Non-Disclosure Agreement (NDA) regarding the content of databases that they manage, and
6. Secured Data Centers must develop and maintain a Data Center Security Policy that lay down the Physical and Administrative Access Policy.

B. TECHNICAL SECURITY MEASURES

1. All desktops that use a database containing personal data shall conform to the guidelines issued by the Information Communication and Technology Management Service (ICTMS), where at the minimum, requires all desktop and laptops to be secured by an Active Directory Login password. All hard drives should be encrypted using the ICTMS approved transparent encryption software, at the minimum, and in the case of a shared desktop, an encrypted working directory;
2. All FOs shall set aside a budget for the upgrading of their data center according to the physical security guideline by the ICTMS;

3. All desktops shall have an encrypted directory. This encrypted directory is exclusively for storing and processing of personal data;
4. Personal data shall be encrypted at all times, starting from the data center, while it is in transit (either via electronic transfer or mobile physical media), and until it is received by the requesting party. ICTMS must study and propose security measures during transit and receiving of personal data by third parties;
5. Prior to the deployment of an online system or database, the concerned OBSUs shall request for the conduct of Vulnerability Assessment Test (VAT) to the ICTMS. Data encryption and installation of security features shall be done to ensure data protection; and
6. All Database applications and systems must use the Access Control List (ACL) specifications of the ICTMS.

The ICTMS shall develop, maintain, and enforce the security protocols necessary to protect the privacy of individuals in its data center.

Data breach is defined as a security violation in which sensitive, protected or confidential data is accessed by unauthorized individuals. The act may include copying, transmitting, viewing, and in some extreme cases, stealing or using data without permission.

Data privacy breach occurs when the database containing personal information and sensitive personal information are:

- Accessed by unauthorized users;
- Unauthorized use, disclosure or disposal of personal information;
- Unauthorized updating or editing of personal information;
- Personal data are lost or stolen during transport;
- Personal information is emailed to the wrong person, and
- Identity theft.

The notion of privacy breach is fluid and may include other violations other than those mentioned above.

A. STEPS IN REPORTING A POSSIBLE DATA PRIVACY BREACH

1. Report the incident to the appropriate Data Protection Officer (DPO)

All personnel are required to immediately report to their respective DPO if they suspect that a policy or any provision of the data protection law is breached.

2. Conduct of Preliminary Incident Assessment by the DPO

Upon receipt of the report, the DPO may call upon the assistance of the ICTMS, Legal Service or equivalent office to assess the situation. All incident reports must be properly documented and assessed. Incident assessment terminates with a final incident assessment report recommending closure or activation of Data Breach Response Team (BRT).

3. Activate the Data Breach Response Team (BRT)

Upon receipt of the final incident assessment report recommending the need for the activation of the BRT, the DPO shall form the BRT team and update the members of the incident. The BRT is tasked to detail out the Breach Management Protocol Plan and submit it to the Personal Information Controller (PIC) and the DPO.

B. ACTIVATING THE BREACH MANAGEMENT PROTOCOL

1. Assessing the Breach

In cases of a personal data breach, the incident shall be recorded in the breach register and reported to the Central Office (CO) PIC and DPO. An assessment shall be conducted and consider the following:

- The circumstances of the possible data breach, including its cause and extent;
- The type or types of personal information involved; and
- Identify all the possible harms to the affected data subjects.

2. Containing the Breach

The BRT shall take immediate action to limit any further access to the affected personal data, e.g., replacing the door locks, taking a system offline, etc.

3. Evaluating the Risk associated with the Breach

The BRT shall assess if the incident caused serious harm to any of the data subjects based on the breach information. The BRT shall notify the affected data subjects immediately upon enough reasonable evidence that the breach is harmful.

A report shall be prepared to the Appointed DPO for transmittal to the National Privacy Commission, giving due consideration to the prescribed timeline. The head of the office where the breach was found, and the DPO must also report the incident to the police or relevant law enforcement agency and request assistance as soon as possible.

4. Restoring Data Integrity

The BRT shall establish if the breach resulted in the loss of data integrity, e.g., possible tampering or alteration of the personal data, erasure, or destruction, in which case, the BRT shall oversee the restoration of the integrity of the records or database.

5. Reviewing and Improving the Security Measures

The BRT shall review and learn from the data breach incident to improve the office's privacy and records management practices. At the minimum, this may include the following:

- A security policy review, back to back with a cause analysis of how the data breach happened;
- Development and presentation of a prevention plan to prevent future incidents;
- A review of policies and procedures and suggest a change(s) to reflect the lessons learned;
- Recommendation on re-training of employee and in extreme case, re-shuffling of employee;
- Review of service delivery partners that were involved in the breach; and
- Include in the regular process audit to ensure the implementation of the prevention plan.

All personnel of the Department shall report and document security incidents and personal data breaches through written reports submitted to the Data Protection Officer (DPO). The DPO shall prepare a formal incident report to the National Privacy Commission (NPC) upon confirmation of a possible breach by the Breach Response Team (BRT). The incident report shall follow the format specified in the NPC circular as follows:

1. Nature of the Breach. This section shall contain the following:

- the nature of the breach;
- a chronology of events; and

- an estimate of the number of affected data subjects.
2. **Personal Data Involved.** This section shall contain a description of the personal data taken.
 3. **Remedial Measures.** This section shall contain the following:
 - Description of the proposed action or action taken to address the breach;
 - Description of actions to secure the remaining data and if possible, detail of actions taken to recover the compromised personal data;
 - Actions performed or proposed to mitigate potential harm or negative consequences, and limit the damage or distress to those affected by the incident;
 - The action being taken to inform the data subjects affected by the event, or reasons for any delay in the notification; and
 - Recommendation on measures to prevent a recurrence of the event.
 4. **Name and contact details.** This section shall contain the contact information of the DPO or contact person(s) designated by the Personal Information Controller (PIC).

These reports shall be submitted to the Appointed DPO and the NPC within 72 hours upon discovery of the incident and the assessment that a personal data breach has occurred. The head of the office where the breach was found and the DPO must also report the incident to the police or relevant law enforcement agency and request assistance as soon as possible.

A. FINAL BREACH INVESTIGATION REPORT

The Department requires the submission of a Final Breach Investigation Report. This report shall contain all findings of the Data Breach Response Team (BRT) and the external authorities participating in the investigation, such as the Philippine National Police, the Local Government Units (LGUs), and the National Bureau of Investigation.

B. PENALTY AND DISCIPLINARY ACTION

Any violation of this Manual shall be subjected to appropriate penalties provided under Republic Act (RA) 10173 or the Data Privacy Act of 2012, and all other pertinent laws, and rules and regulations.

Table 2: Penalties Listed in the RA 10173

Penalties listed in the R.A 10173					
Data Protection Act of 2012 Section	Punishable Act	Jail Term for Personal Information	Jail Term for Sensitive Personal Information	Fine (Pesos) for Personal Information	Fine (Pesos) for Sensitive Personal Information
25	Unauthorized Processing	1-3 years	3-6 years	500k - 2 million	500k - 4million
26	Accessing due to Negligence	1-3 years	3-6 years	500k - 2 million	500k - 4million
27	Improper Disposal	6 months - 2 years	1-3 years	100k - 500k	100k - 1 million
28	Processing for Unauthorized purposes	1 year and 6 months - 5 years	2 - 7 years	500k - 1 million	500k - 2 million
		Jail Term		Fine (Pesos)	
29	Unauthorized Access or Intentional Breach	1-3 years		500k - 2 million	
30	Concealment of Security Breaches	1 year and 6 months - 5 years		500k - 1 million	
31	Malicious Disclosure	1 year and 6 months - 5 years		500k- 1 million	
32	Unauthorized Disclosure	1-3 years	3-5 years	500k - 1 million	500k- 2 million
33	Combination or Series of Acts	3-6 years		1 million - 5 million	

The Department has existing programs, projects and services (PPS) that were developed prior to the passage of Republic Act 10173 or the Data Privacy Act of 2012. This Chapter provides the process in aligning existing PPS with the requirements of the Data Privacy Act of 2012.

A. WHO SHOULD CHAMPION THE ALIGNMENT


The designated Data Protection Officer (DPO), Regional Directors, PPS Director, and the designated PPS DPOs shall initiate and champion the alignment initiative. All existing PPS shall be registered in the Departments' Data Processing System. The PPS will receive its digital data processing registration receipts after a compliance review and evaluation of the NPC.

Upon receipt of the digital certificate, the Data Processing System will be part of the process that will be monitored by the NPC, and part of the Registry of Data Processing System. This shall establish, legalize and legitimize the data processing cycle of the PPS.

B. ALIGNING THE DATA CYCLE WITH THE PRIVACY REQUIREMENTS

The Departments' PPS shall be compliant with the Data Privacy Principles of transparency, legitimate purpose and proportionality. The following steps are essential prior to registration of the data processing system:

1. Review the link between the PPS and the mandate of the Department, laws, or policies which necessitates the development of the PPS.
2. Review, list down, and evaluate the purpose(s) of the PPS. There shall be a clear linkage between the legal basis, the implementation activities, and the purpose(s) of the PPS. This review process shall identify the activities that are outside the scope of the stated purpose of the PPS.
3. Check for the presence of a privacy notice. All existing PPS, including those developed and implemented prior to the passage of the Data Privacy Act, shall have a privacy notice. In its absence, a privacy notice shall be developed and distributed to its beneficiaries to get their consent.
4. Ensure that the data being collected is sufficient and not excessive in relation to the stated purpose.



The Department's Privacy Impact Assessment (PIA) is a two-stage process that prescribes a predefined series of steps in identifying privacy risks. Privacy Risks in general, are normally associated with typical activities which includes, capture, storage, usage, sharing, and destruction of personal data.

A. THE FIRST STAGE PIA PROCESS

GENERAL PRIVACY IMPACT ASSESSMENT

The first PIA shall be conducted during the PPS conceptualization stage. The Department shall refer to it as the General Privacy Impact Assessment. This PIA assessment is necessary for all new PPS of the Department. All PPS must submit their general PIA to the Department's appointed Data Protection Officer (DPO). This shall trigger the submission of the program to the NPC database.

During this stage, the general objectives of the new PPS are set. This stage shall be accomplished by the Program Director and its program DPO. After a thorough review of the result and the risk mitigation plan, the output shall be submitted to the Appointed DPO. The Appointed DPO shall review and register the program and its process to the NPC.

B. THE SECOND STAGE PIA PROCESS

The second PIA is conducted every time there is a data sharing request from a third party. Typically, the process begins early during the development of a partnership or a collaboration proposal from a third party. It is at this stage that the nature of the partnership and the need of a data sharing agreement is explored. The specific purposes of the partnership shall be agreed upon. These specific purposes are the logical outputs that are necessary to attain the general partnership objective(s) or goals.

C. WHO WILL BE RESPONSIBLE IN CONDUCTING THE PIA

The Program/Project Manager or Bureau Director (BD) shall be responsible in ensuring the conduct of PIA every time there is a data sharing agreement. The BD must oversee the PIA process with the program DPO in collaboration and all personnel. This is the first step towards Privacy by Design. In order to achieve this, everyone must be knowledgeable about the efforts to maintain privacy of individual's personal information in our databases.

1. OPERATIONALIZATION OF PROPORTIONALITY

The Principle of Proportionality includes processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose⁷. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means. At this stage, the focus is on the operationalization of proportionality in identifying personal and sensitive data needed to attain the

⁷ IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 10173, ALSO KNOWN AS THE "DATA PRIVACY ACT OF 2012"

purpose/objective. The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

According to the Data Privacy Act, proportionality is defined as:

- a)... data must be specified against an explicit and legitimate purpose
- b) data must be adequate, relevant and not excessive in relation to the purposes for which they are collected
- c)... the data must be accurate and, where necessary, kept up to date at all times.

Only the data that are crucial to the attainment of a specific purpose or objective shall be processed. The DPOs and COPs shall deliberate on the need to process data sets in each purpose or objective. This session shall be facilitated by the Bureau or Program Director.

Table 3: PIA for Data Sharing Assessment Table

Purpose	Objective	Data Needed	Identified Risk	Proposed Risk Mitigation and Cost
<i>Improve Economic Status of the household</i>	<i>Improve income of Household</i>	<ul style="list-style-type: none"> - Number of Income Earner in the HH - identify Income Earners in HH - Last name, first name, type of work - status of work/livelihood - individual's regular/ave. take home - Educational/skills training attainment of each earner 		
	<i>Measure and Monitor HH Livelihood Potential</i>	<ul style="list-style-type: none"> - Educational attainment of each family member - age of each family member - new skill set achieved - increase in income potential. 		

1. Based on the result of the risk assessment, each PPS must design, prepare, and allocate a budget for risk mitigation needed to maintain compliance to the requirements of the privacy law.

2. Every request must be evaluated on the following basis:

- (1) Power and influence of the requesting party;
- (2) Interest of the requesting party;
- (3) Stage of data processing, e.g., during collection, sharing, etc. and
- (4) Number of personal data gathered.

The PIA follows a uniform process and is enumerated as follows:

- Establish the number of personal data to be captured
- Establish the data flow processes
- Conduct Initial Risk Assessment
- Develop the Risk Register
- Develop a Risk Mitigation Plan and Estimate Costs to mitigate
- Implement and Review
- Report the result of the review

Each OBSUs shall have a designated Risk Officer (RO).

2. OPERATIONALIZATION OF TRANSPARENCY

The program DPO and the CPOs shall ensure that the data subject is agreeable to sharing their personal information to third parties while at the same time, ensuring that the following rights of the data subject are observed:

1. **The right to be informed.** Personal data is treated almost literally in the same way as a personal property. It shall not be collected, processed and stored by any organization without the data subject's expressed consent, *unless otherwise provided by law*. Also, data subjects have the right to be informed, in a timely manner, if their data have been compromised.

Through this right, the Department ensures that data subjects are informed of the necessity and reason of data collection, process of data collection and sharing, and instances of data breach.

2. **The right to access.** Data subjects have the right to find out whether an organization holds any personal data and if so, gain "reasonable access" to them.

Through this right, the Department recognizes that a data subject may request for a written description of the kind of information the Department retains pertaining to him or her, and their purpose(s) for retaining them.

3. **The right to object.** The Department recognizes that the data subjects may exercise their right to object if the personal data processing involved is based on consent or on legitimate interest. When the data subject objects or withhold consent, the Department should no longer process the personal data, unless the processing is pursuant to a subpoena, for obvious purposes (contract, employer-employee relationship, etc.) or a result of a legal obligation.
4. **The right to erasure or blocking.** The Department recognizes that data subjects have the right to suspend, withdraw or order the blocking, removal or destruction of their personal data. Data subjects may exercise this right upon discovery and substantial proof of the following:
 - i. The personal data is incomplete, outdated, false, or unlawfully obtained;
 - ii. It is being used for purposes that are not authorized;
 - iii. The data is no longer necessary for the purposes for which they were collected;
 - iv. The data subject decided to withdraw consent, or object to its processing and there is no overriding legal ground for its processing;
 - v. The data concerns information prejudicial to the data subject — unless justified by freedom of speech, of expression, or of the press; or otherwise authorized (by court of law);
 - vi. The processing is unlawful, and
 - vii. The PIC and/or the PIP, violated the data subject rights as a data subject.
5. **The right to damages.** The Department recognized that data subjects may claim compensation if they suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, considering any violation of the rights and freedoms as data subject.
6. **The right to file a complaint with the NPC.** The Department recognizes that the data subject may file a complaint when personal information has been misused, maliciously disclosed, or improperly disposed, or that any of the data subject data privacy rights have been violated.
7. **The right to rectify.** The Department recognizes that data subjects have the right to dispute and have corrected any inaccuracy or error in the data it retains. The Department shall act on it immediately and accordingly, unless

the request is vexatious or unreasonable. Once corrected, the Department shall ensure that the data subject's access and receipt of both new and retracted information. It shall also furnish third parties with said corrected information.

8. **The right to data portability.** The Department recognizes that data subjects have the right to be assured that they remain in full control of their data. Data portability allows the data subject to obtain and electronically move, copy or transfer his or her data in a secure manner, for further use. It enables the free flow of his or her personal information across the internet and organizations, according to the data subject's preference.

Most programs of the Department require the data subject to sign a data sharing consent form at the beginning. This ensures that the program has the authority with regard to sharing personal data with third parties based on the agreed purpose. The only caveat here is that DSWD will only share personal data of its beneficiary when it is towards welfare and development concerns.

3. OPERATIONALIZATION OF LEGITIMACY OF PURPOSE

Data sharing is only allowed if it is towards welfare and development concerns. Any other concern will be subject to legal review and in some extreme cases, as may be determined by the DSWD's DPO, guidance from the NPC must be sought. As of this writing, the DSWD is open to data sharing using its data sharing privilege, when it is about welfare and development concerns.

Parties who wish to enter into a Data Sharing Agreement (DSA) must first convene a meeting to discuss details of their proposed data sharing, which should align to the Data Privacy Principles of transparency, legitimate purpose, and proportionality. They must first clarify the scope of the data sharing agreement; the data to be shared and what not to be shared; designate persons who are to store data and ensure its safety throughout the duration of the agreement; identify when to destroy the data shared, and identify safe physical spaces and infrastructures where data can be stored securely.

Once parties have agreed on the details of this agreement, the drafting of the DSA must follow. Once all parties have signed, the notarized copy of the DSA must be provided to the Legal Service.

Please refer to the *Annexes* for the template of the DSA or NDA and its requirements.



ANNEX A - GENERAL PRIVACY IMPACT ASSESSMENT (NPC PIA TOOLKIT)

PRIVACY IMPACT ASSESSMENT

Overview

A Privacy Impact Assessment (PIA) is an instrument for assessing the potential impacts on privacy of a process, information system, program, software module, device or other initiative which processes personal information and in consultation with stakeholders, for taking actions as necessary to treat privacy risk. A PIA report may include documentation about measures taken for risk treatment, for example, measures arising from the use of the information security management system (ISMS) in ISO/IEC 27001.

A PIA is more than a tool: its process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed. Initiatives vary substantially in scale and impact.

This document is intended to provide scalable guidance that can be applied to all initiatives. Since guidance specific to all circumstances cannot be prescriptive, the guidance in this document should be interpreted with respect to individual circumstance. A Personal Information Controller may have a responsibility to conduct a PIA and may request a Personal Information Processor to assist in doing this, acting on the Personal Information Controller's behalf. A Personal Information Processor or a third party may also wish to conduct their own PIA.

**Privacy Impact Assessment
GUIDE**

I. Project/System Description

a. Description

Describe the program, project, process, measure, system or technology product and its context. Define and specify what it intends to achieve. Consider the pointers below to help you describe the project.

- Brief Description of the project/system
 - Describe the process of the projects
 - Describe the scope and extent
 - Any links with existing programs or other projects
- The system/project's overall aims (purpose of the project/system)
 - What is the project/system aims to achieve?
 - What are the benefits for the organizations and data subjects?
- Any related documents to support the projects/system
 - Project/System Requirements Specification
 - Project/System Design Specification
 - Or any related documents

b. Scope of the PIA

This section should explain, what part or phase of the program the PIA covers and, where necessary for clarity, what it does not cover.

- What will the PIA cover?
- What areas are outside scope?
- Is this just a "desk-top" information gathering exercise, do I have to get information from a wide variety of sources?
- Who needs to be involved and when will they be available?
- Where does the PIA need to fit in the overall project plan and timelines?
- Who will make decisions about the issues identified by the PIA? What information do they need and how long will it take to get sign-off from them?
- Do I need to consult with anyone (for instance the individuals whose personal information the project will involve)? When and how should this happen?
- Are there any third parties involved and how long do I need to allow for them to play their part?

II. Threshold Analysis

The following questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

- a. Will the project or system involve the collection of new information about individuals?

No

Yes

b. Is the information about individuals sensitive in nature and likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?

No Yes

c. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

No Yes

d. Will the initiative require you to contact individuals in ways which they may find intrusive?

No Yes

e. Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?

No Yes

f. Does the initiative involve you using new technology which might be perceived as being privacy intrusive (e.g. biometrics or facial recognition)?

No Yes

g. Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

No Yes

h. Are the personal data collected prior to August 2016?

No Yes

III. Stakeholder(s) Engagement

State all project stakeholders, consulted in conducting PIA. Identify which part they were involved. (Describe how stakeholders were engaged in the PIA process)

Name	Role	Involvement	Inputs/ Recommendations

* add additional rows if needed.

IV. Personal Data Flows

Sample Data Flow

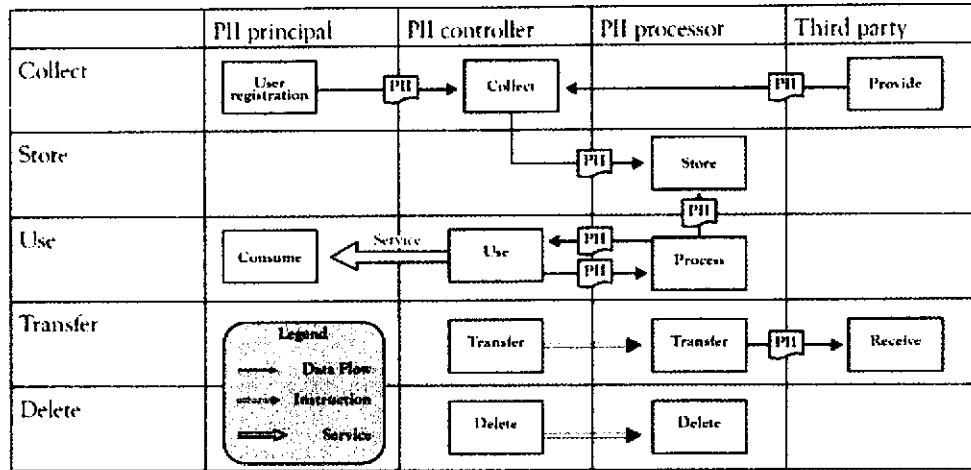


Figure 1. Information flow of personal information can be visualized in a work flow diagram on personal information processing.

- **Objective:** To identify information flows of personal information under assessment.
- **Input:** Description of the process and information system to be assessed.
- **Expected output:** Summary of findings on the information flow of personal information within the process.
- **Actions:** The person responsible for conducting a PIA should consult with others in the organization and perhaps external to the organization to describe the personal information flows and specifically:
 - how personal information is collected and the related source;
 - who is accountable and who is responsible within the organization for the personal information processing;
 - for what purpose personal information is processed;
 - how personal information will be processed;
 - personal information retention and disposal policy;
 - how personal information will be managed and modified;
 - how will personal information processors and application developers protect personal information;
 - identify any personal information transfer to jurisdictions where lower levels of personal information protection apply;
 - whether applicable, notify the relevant authorities of any new personal information processing and seek the necessary approvals.

Output of this process in terms of the information flow of personal information should be documented in the PIA report

- Implementation Guidance:

Use of personal information (or transfer of personal information) may include approved data sharing flows of personal information to other parties.

As an input to the PIA, the organization should describe the information flow in as detailed a manner as possible to help identify potential privacy risks. The assessor should consider the impacts not only on information privacy, privacy related regulations, e.g. telecommunications acts. The whole personal information life cycle should be considered.

Identify the personal data involved and describe the data flow from collection to disposal by answering the following questions below:

What personal data are being or will be processed by this project/system?

List all personal data (e.g. Personal Full Name, address, gender, phone number, etc.) and state which is/ are the sensitive personal information (e.g. race, ethnicity, marital status, health, genetic, government issued numbers).

All the information stated above will be in accordance to the next section.

Collection

1. State who collected or will be collecting the personal information and/or sensitive information.
2. How the personal information/sensitive personal information is collected and from whom it was collected?
 - » If personal information is collected from some source other than the individual?
3. What is/are the purpose(s) of collecting the personal data?
 - » Be clear about the purpose of collecting the information
 - » Are you collecting what you only need?
4. How was or will the consent be obtained?
 - » Do individuals have the opportunity and/or right to decline to provide data?
 - » What happen if they decline?

Storage

1. Where is it currently being stored?
 - » Is it being stored in a physical server or in the cloud?
2. Is it being stored in other country?
 - » If it is subject to a cross border transfer, specify what country or countries.
3. Is the storage of data being outsourced?
 - » Specify if the storing process is being done in-house or is it handled by a service provider

NPC PRIVACY TOOLKIT

Usage

1. How will the data being used or what is the purpose of its processing?
 - » Describe how the collected information is being used or will be used
 - » Specify the processing activities where the personal information is being used.

Retention

1. How long are the data being retained? And Why?
 - » State the length of period the data is being retained!
 - » What is the basis of retaining the data that long? Specify the reason(s)
2. The data is being retained by the organization or is it being outsourced?
 - » Specify if the data retention process is being done in-house or is it handled by a service provider

Disclosure/Sharing

1. To whom it is being disclosed to?
2. Is it being disclosed outside the organization? Why is it being disclosed?
 - » Specify if the personal information is being shared outside the organization
 - » What are the reasons for disclosing the personal information

Disposal/Destruction

1. How will the data be disposed?
 - » Describe the process of disposing the personal information
2. Who will facilitate the destruction of the data?
 - » State if the process is being managed in-house or if it is a third party

V. Privacy Impact Analysis

Each program, project or means for collecting personal information should be tested for consistency with the following Data Privacy Principles (as identified in Rule IV, Implementing Rules and Regulations of Republic Act No. 10173, known as the "Data Privacy Act of 2012"). Respond accordingly with the questions by checking either the "Yes" or "No" column and/or listing the what the questions may indicate.

Transparency	Yes	No	Not applicable
1. Are data subjects aware of the nature, purpose, and extent of the processing of his or her personal data?			
2. Are data subjects aware of the risks and safeguards involved in the processing of his or her personal data?			

<p>3. Are data subjects aware of his or her rights as a data subject and how these can be exercised? Below are the rights of the data subjects:</p> <ul style="list-style-type: none"> ✓ Right to be informed ✓ Right to object ✓ Right to access ✓ Right to correct ✓ Right for erasure or blocking ✓ Right to file a complaint ✓ Right to damages ✓ Right to data portability 			
<p>4. Is there a document available for public review that sets out the policies for the management of personal data?</p> <p><i>Please identify document(s) and provide link where available:</i></p> <p>_____</p> <p>_____</p>			
<p>5. Are there steps in place to allow an individual to know what personal data it holds about them and its purpose of collection, usage and disclosure?</p>			
<p>6. Are the data subjects aware of the identity of the personal information controller or the organization/entity processing their personal data?</p>			
<p>7. Are the data subjects provided information about how to contact the organization's Data Protection Officer (DPO)?</p>			
<p>Legitimate Purpose</p>	<p>Yes</p>	<p>No</p>	<p>Not applicable</p>
<p>1. Is the processing of personal data compatible with a declared and specified purpose which are not contrary to law, morals, or public policy?</p>			
<p>2. Is the processing of personal data authorized by a specific law or regulation, or by the individual through express consent?</p>			
<p>Proportionality</p>	<p>Yes</p>	<p>No</p>	<p>Not applicable</p>
<p>1. Is the processing of personal data adequate, relevant, suitable, necessary and not excessive in relation to a declared and specified purpose?</p>			
<p>2. Is the processing of personal data necessary to fulfill the purpose of the processing and no other means are available?</p>			

Collection	Yes	No	Not applicable
1. Is the collection of personal data for a declared, specified and legitimate purpose?			
2. Is individual consent secured prior to the collection and processing of personal data? If no, specify the reason _____			
3. Is consent time-bound in relation to the declared, specified and legitimate purpose?			
4. Can consent be withdrawn?			
5. Are all the personal data collected necessary for the program?			
6. Are the personal data anonymized or de-identified?			
7. Is the collection of personal data directly from the individual?			
8. Is there authority for collecting personal data about the individual from other sources?			
9. Is it necessary to assign or collect a unique identifier to individuals to enable your organization to carry out the program?			
10. Is it necessary to collect a unique identifier of another agency? <i>e.g. SSS number, PhilHealth, TIN, Pag-IBIG, etc.</i>			
Use and Disclosure	Yes	No	Not applicable
1. Will Personal data only be used or disclosed for the primary purpose?			
2. Are the uses and disclosures of personal data for a secondary purpose authorized by law or the individual?			

Data Quality	Yes	No	Not applicable
1. Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.1 *Please identify all steps taken to ensure that all data that is collected, used or disclosed will be accurate, complete and up to date:			
1.2 *The system is regularly tested for accuracy			
1.3 *Periodic reviews of the information			
1.4 *A disposal schedule in place that deletes information that is over the retention period			
1.5 *Staff are trained in the use of the tools and receive periodic updates			
1.6 *Reviews of audit trails are undertaken regularly			
1.7 *Independent oversight			
1.8 *Incidents are reviewed for lessons learnt and systems/ processes updated appropriately			
1.9 *Others, please specify _____ _____			
Data Security	Yes	No	Not applicable
1. Do you have appropriate and reasonable organizational, physical and technical security measures in place? <i>organizational measures - refer to the system's environment, particularly to the individuals carrying them out. Implementing the organizational data protection policies aim to maintain the availability, integrity, and confidentiality of personal data against any accidental or unlawful processing (i.e. access control policy, employee training, surveillance, etc.,)</i> <i>physical measures - refers to policies and procedures shall be implemented to monitor and limit access to and activities in the room, workstation or facility, including guidelines that specify the proper use of and access to electronic media (i.e. locks, backup protection, workstation protection, etc.,)</i> <i>technical measures - involves the technological aspect of security in protecting personal information (i.e. encryption, data center policies, data transfer policies, etc.,)</i>			

Organizational Security	Yes	No	Not applicable
*Have you appointed a data protection officer or compliance officer?			
*Are there any data protection and security measure policies in place?			
*Do you have an inventory of processing systems? Will you include this project/system?			
*Are the users/staffs that will process personal data through this project/system under strict confidentiality if the personal data are not intended for public disclosure?			
*If the processing is delegated to a Personal Information Processor, have you reviewed the contract with the personal information processor?			
Physical Security	Yes	No	Not applicable
*Are there policies and procedures to monitor and limit the access to this project/system?			
*Are the duties, responsibilities and schedule of the individuals that will handle the personal data processing clearly defined?			
*Do you have an inventory of processing systems? Will you include this project/system?			
Technical Security	Yes	No	Not applicable
*Is there a security policy with respect to the processing of personal data?			
*Do you have policies and procedures to restore the availability and access to personal data when an incident happens?			
*Do/Will you regularly test, assess and evaluate the effectiveness of the security measures of this project/system?			
*Are the personal data processed by this project/system encrypted while in transit or at rest?			

2. The program has taken reasonable steps to protect the personal data it holds from misuse and loss and from unauthorized access, modification or disclosure?			
3. If yes, which of the following has the program undertaken to protect personal data across the information lifecycle:			
3.1 * Identifying and understanding information types			
3.2 * Assessing and determining the value of the information			
3.3 * Identifying the security risks to the information			
3.4 * Applying security measures to protect the information			
3.5 * Managing the information risks.			
Disposal	Yes	No	Not applicable
1. The program will take reasonable steps to destroy or de-identify personal data if it is no longer needed for any purpose. <i>If YES, please list the steps</i> _____ _____			
Cross-border Data Flows (optional)	Yes	No	Not applicable
1. The program will transfer personal data to an organization or person outside of the Philippines <i>If YES, please describe</i> _____ _____			
2. Personal data will only be transferred to someone outside of the Philippines if any of the following apply: a. The individual consents to the transfer b. The organization reasonably believes that the recipient is subject to laws or a contract enforcing information handling principles substantially similar to the DPA of 2012 c. The transfer is necessary for the performance of a contract between the individual and the organization d. The transfer is necessary as part of a contract in the interest of the individual between the organization and a third party e. The transfer is for the benefit of the individual;			

NPC PRIVACY TOOLKIT

<p>3. The organization has taken reasonable steps so that the information transferred will be stored, used, disclosed and otherwise processed consistently with the DPA of 2012 If YES, please describe</p> <hr/> <hr/>			
---	--	--	--

VI. Privacy Risk Management

For the purpose of this section, a risk refers to the potential of an incident to result in harm or danger to a data subject or organization. Risks are those that could lead to the unauthorized collection, use, disclosure or access to personal data. It includes risks that the confidentiality, integrity and availability of personal data will not be maintained, or the risk that processing will violate rights of data subjects or privacy principles (transparency, legitimacy and proportionality).

The first step in managing risks is to identify them, including threats and vulnerabilities, and by evaluating its impact and probability.

The following definitions are used in this section,

Risk - "the potential for loss, damage or destruction as a result of a threat exploiting a vulnerability";

Threat - "a potential cause of an unwanted incident, which may result in harm to a system or organization";

Vulnerability - "a weakness of an asset or group of assets that can be exploited by one or more threats";

Impact - severity of the injuries that might arise if the event does occur (can be ranked from trivial injuries to major injuries); and

Probability - chance or probability of something happening;

Impact		
Rating	Types	Description
1	Negligible	The data subjects will either not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2	Limited	The data subject may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3	Significant	The data subjects may encounter significant inconveniences, which they should be able to overcome but with serious difficulties.
4	Maximum	The data subjects may encounter significant inconveniences, or even irreversible, consequences, which they may not overcome.

**ANNEX B - TEMPLATE FOR DATA SHARING AND NON-DISCLOSURE
AGREEMENT**

Data Sharing Agreement
between the
Department of Social Welfare and Development (DSWD)
and the
(Name of Second Party / AGENCY / LGU).

KNOW ALL MEN BY THIS PRESENTS:

This Memorandum of Agreement, hereinafter referred to as MOA or Agreement, made and entered into this _____ day of _____ at Quezon City, Philippines, by and between:

The **DEPARTMENT OF SOCIAL WELFARE AND DEVELOPMENT (DSWD)**, a national government agency created and existing under the laws of the Republic of the Philippines with principal office address at Batasang Pambansa Complex, Constitution Hills, Quezon City herein represented by _____ in his/her capacity as the _____, and hereinafter referred to as **First Party**;

and

The (Name of second party), (Description of agency/organization) with office address (Please state) herein represented by (Please state) in his/her capacity as (Please state), and hereinafter referred to as **Second Party**;

WHEREAS, the Philippine Constitution declares that the State shall promote a just and dynamic social order that will ensure the prosperity and independence of the nation and free the people from poverty through policies that provide adequate social services, promote full employment, a rising standard of living, and an improved quality of life for all;

WHEREAS, the **First Party** is mandated under the Administrative Code of 1987 to provide a balanced approach to welfare whereby the needs and interests of the population are addressed not only at the outbreak of crisis but more importantly at the stage which would inexorably lead to such crisis, which strategy requires providing an integrated welfare package to its constituents on the basis of their needs and coordinating the service facilities required from such Departments or agencies, governmental and non-governmental, which can best provide them;

WHEREAS, in order to fulfill its mandate and objectives, the Administrative Code of 1987 directs the **First Party** to formulate, support, develop and implement plans and projects in the field of social welfare and development, identify and deliver appropriate interventions, provide consultative and information services to institutions and organizations involved in social welfare activities;

WHEREAS, the **First Party** is mandated to provide assistance to other national government agencies (NGAs), local government units (LGUs), non-government organizations (NGOs), people's organizations (POs), and members of civil society in the implementation of programs, projects and services that will assist the

disadvantaged individuals, families and communities during National State of Emergency or Calamity;

WHEREAS, Section 22 of Republic Act No. 10173 provides that all sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the National Privacy Commission (NPC), and that the head of each government agency or instrumentality shall be responsible for complying with the security requirements provide under the Data Privacy Act of 2012;

WHEREAS, NPC Circular 16-02 provides the rules governing data sharing agreements involving government agencies;

WHEREAS, (insert mandate of particular NPMO/Office who will release the data).

WHEREAS, the **Second Party** is mandated to _____ (Please state) _____;

WHEREAS, the **Second Party** shall implement the social protection programs and services defined in Annex A and be allowed secured access to (DSWD Database) data maintained by the First Party;

NOW THEREFORE, for and in consideration of the above premises, the **Parties** hereby agree as follows:

Definitions

For the purposes of this MOA, "personal data", "personal information controller", "process/processing", "data subject" and "data sharing" shall have the same meaning as in Republic Act No. 10173 or the Data Privacy Act of 2012, and its Implementing Rules and Regulations.

Specific Purpose of the Data Sharing:

1. ...

** Note: as a best practice, it is recommended that the specific purpose(s) as determined and agreed on by both parties through the use of the guide table presented in the manual be enumerated here.*

In so doing, the agreement clearly demonstrates the program/projects adherence to the three principles of privacy, transparency, proportionality and legitimacy of purpose.

Obligations of the First Party

The First Party shall:

2. Act as and have the duties and accountabilities of a personal information controller for all personal data processed by (DSWD OBSU);

3. Have in place reasonable and appropriate physical, technical and organizational measures intended to protect personal data up to the date of transfer to the Second Party, against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, as well as against any other unlawful processing;
4. Uphold the rights of the data subject in accordance with RA No. 10173 and relevant rules;
5. Have in place the required procedures or protocols so that any person or party acting under the authority of the First Party to have access to the personal data for transfer will respect and maintain the confidentiality and security of the personal data, and shall be obligated to process the personal data only on instructions from the First Party;
6. Process and transfer personal data to the Second Party in accordance with the Data Privacy Act, DSWD data sharing protocol, which includes privacy policies and guidelines, and the details of the transfer specified in Annex A of this Agreement;
7. Provide the Second Party, when so requested, with information vital to the proper use and protection of the shared data, particularly on relevant stipulations under the Data Privacy Act and DSWD data sharing and privacy policies and guidelines;
8. Respond, within reasonable time, to information requests and complaints from data subjects and the NPC concerning processing of the personal data by the Second Party to the extent reasonably possible and with the information reasonably available to it if the Second Party is unwilling and unable to respond;
9. Make available, upon request and following the procedures laid out in DSWD data sharing and privacy policies and guidelines, a copy of this Agreement to the affected data subjects, as well as the NPC where required; and
10. Provide the Second Party with a password that will be used to access encrypted DSWD data (DSWD OBSU eg. Soc Pen, UCT, Listahanan, Pantawid etc.); **Provided that** only the Second Party, through its authorized staff enumerated in Annex A, will use such a password.

Obligations of the Second Party

The Second Party shall:

1. Act as and have the duties and accountabilities of a personal information controller for all personal data received from the First Party and covered under this Agreement;

2. Have in place appropriate physical, technical and organizational measures to protect the personal data received from the First Party against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, as well as against any other unlawful processing;
3. Uphold the rights of the data subject in accordance with RA No. 10173 and relevant rules;
4. Receive and further process personal data from the First Party in accordance with RA No. 10173 and the data sharing and privacy policies and guidelines of the First Party, and for purposes described in Annex A;
5. Have the legal authority to give warranties and fulfill the undertakings set out in this Agreement;
6. Have in place the required procedures or protocols so that any person or party acting under the authority of the Second Party to have access to the personal data will be legally answerable to the Second Party to respect and maintain the confidentiality and security of the personal data, and shall be obligated to process the personal data only on instructions from the Second Party;
7. **Not disclose or transfer the personal data to a third party, except those disclosures authorized by law, or provided that such transfer or disclosure of personal data to be made by the Second Party to a third party personal information controller will be:**
 - a. the **sole responsibility of the Second Party** as a personal information controller, and therefore, the **transferred personal data will no longer be the accountability or liability of the First Party;**
 - b. compliant to the Data Privacy Act, its IRR and other relevant laws, and executed with adequate safeguards in place for the protection of personal data; and that any infringement against this obligation or applicable law may result in serious fines under RA 101173, its IRR and other guidelines and circulars issued by the NPC, and
 - c. Covered by a separate agreement in accordance to the mandates of the Data Privacy Act of 2012;

Furthermore, the Second Party ensures that personal data:

- are processed only according to the extent required;
- are always accurate and, where necessary, kept up to date;
- are kept for no longer than is necessary for the purposes for collecting the said personal data;
- are processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful access or processing and accidental loss, destruction or damage, using appropriate physical, technical and organizational measures in accordance with the specification of the appropriate Law.

- d. The Second Party commits to observe the strictest confidentiality concerning the personal data it shall collect, process, or access to in the performance of its duties and functions, and refrain from disclosing them to any other natural or legal person, including among its workers and other staff, not expressly authorized to access the personal data. This non-disclosure and confidentiality obligation shall stay unaffected without limitation in time, even in the case of resignation or termination from employment, end of term or appointment of the Second Party's authorized personnel or officer handling such data.
8. Have no reason to believe, at the time of entering into this MOA, in the existence of any laws that would have a substantial adverse effect on the guarantees provided for under this Agreement, and it will inform the First Party if it becomes aware of any such laws;
9. Identify to the First Party a designated data protection officer within its organization authorized to respond to information requests and complaints concerning processing of the personal data, and will cooperate in good faith with the First Party, the data subject and the NPC concerning all such enquiries within a reasonable time;
10. Upon reasonable request of the First Party, submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certification by the NPC to ascertain compliance with the warranties and undertakings in this MOA, with reasonable notice and during regular business hours;
11. Provide the First Party with information necessary for the sharing of personal data, including but not limited to specific data requirements, processes to be applied to the personal data, timeframe as to when the said data will be needed, and the list of names of the staff and respective position titles who will be authorized to access DSWD data Social Pension Database, and which shall form part of the details of transfer in Annex A, and;
12. Accomplish the feedback report form on data utilization as provided by the First Party.

General Provision

The Parties agree that the provisions of RA No. 10173 shall be considered read into this Agreement and that the same principles of transparency, legitimate purpose and proportionality shall govern the implementation of this Agreement

Termination of Agreement

This MOA shall automatically be deemed terminated at the (***state duration or period of State of Emergency or termination period e.g. __ days upon lifting of State of Emergency***). Either party may also be entitled to terminate the MOA in the event of any breach of obligations under the same. The parties agree,

however, that the termination of the Agreement at any time, in any circumstances and for whatever reason, does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

In the event of termination of this MOA, the Second Party must securely return all personal data and all copies of the personal data subject to this Agreement to the First Party forthwith or, at the First Party's choice, will destroy all copies of the same according to the requirement for disposal stipulated in RA 10173. The Second Party certifies to the First Party that it has returned all copies or has destroyed the data as stipulated, unless the Second Party is prevented by law from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose.

Description of the Transfer

The details of the transfer and of the personal data are specified in Annex A, which forms an integral part of this MOA. The parties may execute additional annexes to cover additional transfers, which will be submitted to the NPC where required. Annex A may, in the alternative, be drafted to cover multiple transfers.

Liabilities

Each party shall be liable for the violation of pertinent provisions of RA10173, and may be penalized as stipulated in Sections 25-37, Chapter VIII of the Act. The parties agree that they may be exempted from this liability upon proving that neither of them is responsible for the said violation.

Breach of any clause of this Agreement, and provisions of the data sharing and privacy policy and guidelines of the First Party shall mean the immediate termination of the MOA and the blacklisting of the Second Party from further usage of any data from (DSWD / DSWD OBSU).

The Second Party further agrees to indemnify the First Party against all costs, claims, damages or expenses incurred by the First Party or for which the First Party may become liable due to any failure by the Second Party or its employees, subcontractors or agents, and any other party receiving the personal data from the Second Party, to comply with the obligations under this Agreement.

Resolution of Disputes with Data Subjects

The Parties agree that a data subject shall have the right to enforce his or her rights as stipulated in RA 10173 against either Party, for their respective breach of their contractual obligations, with regard to the data subject's personal data. In cases involving allegations of breach by the Second Party, the data subject must first directly enforce his or her rights against the Second Party. If the Second Party does not take appropriate action within a reasonable period (which under normal circumstances would be one month) the data subject may then request the First Party to take appropriate action to enforce his or her rights against the Second Party.

In the event of a dispute or claim brought by a data subject concerning the processing of the personal data against either or both of the Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

The Parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed by the NPC for data protection disputes.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be signed in their respective names in _____, Republic of the Philippines, as of the day and year written above:

For the Department of Social Welfare and Development (DSWD)	For the SECOND PARTY (Specify the Name)
---	--

(Authorized Representative)		(Authorized Representative)

[Important Note: *Should the signing authority on behalf of the NGA/ LGU is not the Head of Agency or the Local Chief Executive, the requesting party must submit a written document that would show authority of the designated signatory.*]

Signed in the Presence of:

(DSWD Designated Data Protection Officer)		(NGA / LGU Designated Data Protection Officer)

[Note: *Written document must be submitted by the NGA / LGU showing the official designation of the LGU Data Protection Officer.*]

ANNEX A: Description of the Transfer

(Please accomplish this form accurately and exhaustively. Do not be limited by the spaces provided. You may use additional sheets if necessary.)

DATA SUBJECTS

The personal data transferred concern the following categories of data subjects *(Please specify)*:

PURPOSES OF THE TRANSFER

The transfer is made for the following purposes *(Please provide detailed information)*:

CATEGORIES OF DATA

The personal data transferred concern the following categories of data *(Please specify the type of personal data)*:

ADDITIONAL USEFUL INFORMATION

(Describe arrangements for securing password, storage limits and other relevant information)

SECOND PARTY (e.g. LGU) DESIGNATED DATA HANDLERS OTHER THAN DATA PROTECTION OFFICER

(Specific names of Designated Staff and their specific roles and responsibilities such as those assigned to handle, process, store, delete data within the specified timeline)

DESIGNATED DATA PROTECTION OFFICERS

First Party	Second Party
<hr/> (Name)	<hr/> (Name)
<hr/> (Position)	<hr/> (Position)

ANNEX B

B – 1: AUTHORITY OF DESIGNATED SIGNATORY

[Note: Should the signing authority on behalf of the LGU is not the Local Chief Executive, the requesting party must submit a written document that would show authority of the designated signatory.]

B – 2: AUTHORITY OF DESIGNATED DATA PROTECTION OFFICER

ACKNOWLEDGMENT
REPUBLIC OF THE PHILIPPINES)
_____) S.S.

BEFORE ME, a Notary Public for and in the above jurisdiction, personally appeared the following:

NAME	VERIFIED EVIDENCE OF IDENTITY	DATE/PLACE ISSUED
------	-------------------------------	-------------------

(Name of First Party)

(Name of Second Party)

known to me to be the named persons who executed the foregoing instrument and acknowledged to me that the same is their own free will and voluntary act and deed.

This instrument consists of ten (10) pages including this page wherein this Acknowledgment is written, and is signed by the parties and their instrumental witnesses on each and every page hereof.

WITNESS MY HAND AND SEAL, this _____ day of _____ 20____
at _____, Philippines.

NOTARY PUBLIC

Doc. No. _____:
Page No. _____:
Book No. _____:
Series of 20__

ANNEX C - TEMPLATE FOR BREACH REPORTING

BREACH INCIDENT REPORT TEMPLATE

Notification Type:

Date of Submission	
Contact Person (COP/ DPO)	
Email Address and Contact Person	
OBSUS	
Date of Occurrence	
Date of Discovery	
Date of Notification	
Brief Summary	
Involves SPI or data that may enable identity Fraud	YES NO
Acquire by an unauthorized person	YES NO
Likely to give rise to a real risk of serious harm to data subjects	YES NO

Personal Data Breach Notification Details:

Sector Name	
Sub Sector Name	
General Cause	Malicious Attack System Glitch Human Error Malicious Attack/ System Glitch Malicious Attack/ Human Error System Glitch/ Human Error
Specific Cause	Hacking-Cloud Hacking-Database Hacking-Email Account Hacking-Infrastructure Hacking-Server Hacking-Website Hacking-Others Theft Social Engineering

	Malware-Ransomware Malware-Trojan Horse Hacking-SQL Injection Phishing Smishing Hacking-Phishing Malware-Virus Hacking-Man-In-The Middle Others: _____
--	--

With Request⁸:

- YES
- NO

1.a. How breach occurred + DPS Vulnerability

(Description on how the breach occurred and the vulnerability of the data processing system that allowed the breach.)

1.b Chronology

1.c. Number of DS/Records

(Approximate number of data subjects or records involved.)

No. of:

Provide Details:

1.d. Description/Nature

(An availability breach resulting from loss, accidental or unlawful destruction of personal data; Integrity breach resulting from alteration of personal data; and/ or a confidentiality breach resulting from the unauthorized disclosure of or access to personal data)

⁸ Refers to request for postponement of data subject notifications, alternative means, etc. (Refer to NPC 16-03)

1.e. Likely Consequences

(Provide how the incident will affect both the Personal Information Controller and its data subjects.)

2.a. SPI

(Sensitive personal 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.)*

2.b. Other info that may enable identity fraud

(Data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.)

3.a. Measures to address the breach

(Specific measures taken to address the incident including the results of the investigation conducted.)

3.b. Measures to secure/recover personal data

[Empty box for measures to secure/recover personal data]

3.c. Actions to Mitigate Harm

[Empty box for actions to mitigate harm]

3.d. Actions to Inform Data subjects

[Empty box for actions to inform data subjects]

3.e. Measures to prevent recurrent of incidence

[Empty box for measures to prevent recurrent of incidence]

Record Type:

Digital Records in Electronic Systems
Digital Records in Email
Digital Records in Removable Media or Portable Device
Physical Records

Data Subjects:

Own Employees
Customers
Personal Data of Vulnerable Groups
Others

MANDATORY BREACH NOTIFICATION TO DATA SUBJECT TEMPLATE

<NAME OF ENTITY>
<ADDRESS>
<CONTACT INFORMATION>

<DATE>

<DATA SUBJECT>
<ADDRESS>

Subject: <DATA BREACH> dated <DATE>
<NPC REGISTRATION NO.>

Dear <DATA SUBJECT>

I write in behalf of <ENTITY>, regarding your data in <BRIEF DESCRIPTION OF DATABASE>.

We regret to inform you that your data has been exposed in this data breach. To our understanding, your exposure is limited to: <DATA INVOLVED IN THE DATA BREACH>.

Nature of the Breach

- Provide a summary of the events that led up to the loss of control over the data. Do not further expose the data subject.
- Describe the likely consequences of the personal data breach.

Measures taken to Address the Breach.

- Provide information on measures taken or proposed to be taken to address the breach, and to secure or recover the personal data that were compromised.
- Include actions taken to inform affected individuals of the incident. In case the notification has been delayed, provide reasons.
- Describe steps the organization has taken prevent a recurrence of the incident.

Measures taken to reduce the harm or negative consequences of the breach.

- Describe actions taken to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.

Assistance to be provided to the affected data subjects.

- Include information on any assistance to be given to affected individuals.

Do not hesitate to contact our Data Protection Officer for further information:

Data Protection Officer <DATA PROTECTION OFFICER>
<OFFICE ADDRESS>
<E-MAIL ADDRESS>

<TELEPHONE>
<OTHER CONTACT INFORMATION>

We undertake to provide more information to you as soon as they become available.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/>

ANNUAL SECURITY INCIDENT REPORT TEMPLATE FOR PIC

SUMMARY
Annual Security Incident Reports
January to December 2017

Sector: _____ City/Municipality: _____ Province: _____

PIC (Individual or Organization) _____

Name of DPO _____

PERSONAL INFORMATION CONTROLLER

A. Personal Data Breach, Mandatory Notification	<#>
B. Personal Data Breach, not covered by mandatory notification requirements	<#>
C. Other Security Incidents	<#>
D. Total Security Incidents (D = A+B+C)	<#>

How Security Incidents Occurred

Types	Number	Types	Number
Theft	<#>	Communication Failure	<#>
Fraud	<#>	Fire	<#>
Sabotage/Physical Damage	<#>	Flood	<#>
Malicious Code	<#>	Design Error	<#>
Hacking/Logical Infiltration	<#>	User Error	<#>
Misuse of Resources	<#>	Operations Error	<#>
Hardware Failure	<#>	Software Maintenance Error	<#>
Software Failure	<#>	Third Party Services	<#>
Hardware Maintenance Error	<#>	Others	<#>

Personal Data Breaches

	Confidentiality	Integrity	Availability
Mandatory Notification Required	<#>	<#>	<#>
Mandatory Notification Not Required	<#>	<#>	<#>

PREPARED BY : _____ E-MAIL: _____

DESIGNATION : _____ CONTACT NO.: _____

DATE : _____

ANNEX D DSWD DATA CONSENT FORM

DSWD DATA CONSENT FORM

This is to notify you that the Department of Social Welfare and Development (DSWD) collect, store, use, and process necessary data in order to collaborate with Social Welfare and Development partners readily, other National Government Agencies (NGAs), and Local Government Units (LGUs) automatically.

This form also ensures that data subjects that the DSWD shall be responsible through the Personal Information Controller or Data Processor shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of any information processed to protect personal data against accidental, unlawful destruction, unexpected loss, alteration, unauthorized disclosure, access, and any other prohibited forms of processing.

I have read and understood the Data Collection Form of the DSWD and express my consent thereto. I hereby provide my right to be informed, access, rectification, erasure, object and file a complaint if any privacy rights have been violated pursuant to the provisions of the Republic Act No. 10173 also known as the Data Privacy Act of 2012

(Signature over Printed Name)

(Date)