

OFFICE OF THE PRESIDENT OF THE PHILIPPINES
Office of the Presidential Adviser on the Peace Process



Data Privacy Manual



TABLE OF CONTENTS

I. Introduction	1
II. Definition of Terms	1
III. Governing Policies and Programs	2
IV. Scope and Limitation	3
V. Personal Data and Information Processing	3
VI. Security Measures	11
VII. Breach and Security Incidents	22
VIII. Inquiries and Complaints	25
IX. Annexes	26

LIST OF TABLES

Table 1. OPAPP Personal Data and Information Classification, and Authority of Access	6
Table 2. External and Internal Data Sharing Requirements	10
Table 3. OPAPP PIA Process and Timeline	12
Table 4. Proposed Trainings and Seminars and Target Beneficiaries	16
Table 5. Data and Information Management Measures	17

LIST OF FIGURES

Figure 1. Security Incident Management Flow	23
Figure 2. Privacy Security Incidents and Breaches Reporting Structure	23

I. INTRODUCTION

Since its establishment, the Office of the Presidential Adviser on the Peace Process (OPAPP), has made notable milestones in developing policies, and implementing programs, projects, and activities for conflict-affected and conflict-vulnerable areas with the utmost respect for, and ensuring we are able to nurture relationships of trust, accountability, and confidence among our stakeholders. As part of our continuous efforts to uphold the General Data Privacy Principles of transparency, legitimate purpose, and proportionality, OPAPP has endeavored to protect personal data and information through the identification of programs, processes and systems that collect and process personal information, risk assessments, privacy policy development, and the conduct of orientations on data security and cybersecurity.

In furtherance of the aim to provide uninterrupted and robust data privacy protection services to the organizational assets, OPAPP, in compliance to the Republic Act 10173 or the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR), and other relevant policies, including issuances of the National Privacy Commission (NPC), shall adopt and implement this Privacy Manual. This Manual shall inform OPAPP personnel and data protection officers of the organization's data protection and security measures, building and nurturing a culture that values and promotes the right to privacy.

II. DEFINITION OF TERMS¹

A. Data Protection Officer

The official of OPAPP who has independent and autonomous jurisdiction and authority over data and information protection and data privacy matters.

B. Data Subject

This refers to an individual whose personal, sensitive-personal, or privileged information is processed.

C. Personal Data

This refers to all types of personal information, including privileged information.

D. Personal Information

This 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.

¹ R.A. 10173 s. 2012 Section 3., "Definition of Terms", and IRR Rule I, "Preliminary Provisions"

E. Personal Information Controller

This refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

1. a person or organization who performs such functions as instructed by another person or organization; or
2. an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

3. Personal Information Processor (PIP)

This refers to any natural or juridical person qualified to act as such under DPA to whom a PIC may outsource the processing of personal data pertaining to a data subject.

4. Privacy Impact Assessment

A process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, activity, process or measure.

5. Personal Data and Information Processing

This refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

III. GOVERNING POLICIES AND PROGRAMS

All processing of personal data and information within OPAPP shall be governed by the following policies:

- A.** R.A. 10173 "Data Privacy Act of 2012"
- B.** R.A. 9470 "The National Archives of the Philippines Act of 2007"
- C.** E.O. 2, s. 2016 "Operationalizing in the Executive Branch the People's Constitutional Right to Information and the State Policies to Full Public Disclosure and Transparency in the Public Service and Providing Guidelines Therefore."
- D.** Memorandum from the Executive Secretary dated 24 November 2016, "Inventory of Exceptions to E.O. 2 s. 2016"
- E.** E.O. 608, s. 2007 "Establishing a National Security Clearance System for Government Personnel with Access to Classified Matters and for Other Purposes"
- F.** ISO/IEC 27001 International Standard on Information Security Management
- G.** ISO/IEC 27701 International Standard on Personal Identifiable Information (PII)

- H. ISO 27032 International Standard on Cybersecurity Management
- I. ISO 31000 International Standard on Risk Management
- J. ISO 22301 International Standard on Business Continuity Management System (BCMS)
- K. OPAPP Privacy Management Framework
- L. Policies, Guidelines, and Frameworks of OPAPP
- M. Laws and Regulations that may repeal the foregoing.

IV. SCOPE AND LIMITATION

This Manual shall govern the overall operations of OPAPP, as well as acts and decisions of its partners, clients, stakeholders, outsources, subcontractors, licensors, licensees, donors, beneficiaries, resource persons, consultants, job orders, contractual and permanent employees and officers, retirees, former employees, applicants, contract counterparties, and other persons whose personal data are directly or indirectly processed by OPAPP and its departments and area management offices (collectively called as “OPAPP Data Subjects”).

V. PERSONAL DATA AND INFORMATION PROCESSING

OPAPP, its departments and area management offices, processes personal data and information in accordance to its mandate to oversee, coordinate, and integrate the implementation of the comprehensive peace process, other policy issuances, and as a national government agency.

A. Principles of Processing Personal Data and Information²

OPAPP shall process personal data and information subject to the requirements of the Data Privacy Act of 2012 and other laws allowing disclosure of information to the public, and adherence to the following principles:

1. **Transparency** – OPAPP shall ensure that the Data Subjects are aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, their rights as data subjects and how these can be exercised.
2. **Legitimate purpose** – OPAPP shall ensure that the processing of personal data and information is compatible with a declared and specified purpose which must not be contrary to law, morals or public policy.
3. **Proportionality** – OPAPP shall ensure that the processing of personal data and information is adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

B. Purposes of Processing Personal Data and Information³

OPAPP processes personal data and information using one or more of the following grounds:

² R.A. 10173, IRR, Rule No. 4 “Data Privacy Principles”

³ R.A. 10173, IRR, Rule No. 5 “Lawful Processing of Personal Data”

1. Performance of the agency's obligations and deliverables in accordance to its mandates as a national government agency pursuant to Executive Order 125, s. 1993, as amended by Executive Order 3, s. 2001.
2. Protection of privacy rights and welfare of OPAPP Data Subjects in accordance to the RA 10173 or the Data Privacy Act of 2012 and other policy issuances of the NPC.
3. Overall internal and external operational management as a national government agency and Personal Information Controller.

In accordance to the abovementioned, OPAPP processes personal data and information for the following purposes:

1. Delivery of services to conflict-affected and conflict-vulnerable areas through the agency's programs, projects, and activities;
2. Overall operational management of OPAPP departments and area management offices, including administrative and technical operations, among others;
3. Management of human resources, including external sources of technical service providers and prospective human resources;
4. OPAPP data subjects external and internal affairs and relations;
5. Database and records keeping and maintenance;
6. Research and documentations;
7. Media coverage;
8. Corporate and governance requirements and due diligence;
9. Partnerships, donors' management, and external relations; and
10. Any other activities that may require the processing of personal data and information.

C. Privacy Notice for the General Public

A General Privacy Notice contains the list of OPAPP's services, types of personal data and information being processed, methods and timing of collection, purposes of processing personal data and information, processing activities, summary of data and information security measures in place, rights of the data subjects, and inquiry platforms (**See Annex A for the Privacy Notice.**) The Notice shall be uploaded in OPAPP's website, official social media accounts, as well as all systems designed to generate and process personal data and information. A summarized general privacy notice shall also be included in all activities which will process personal data and information. This may include recorded online meetings, online survey forms/registration forms, and physical/face-to-face activities, among others. The summarized privacy notice shall read:

The Office of the Presidential Adviser on the Peace Process (OPAPP), mandated to oversee, coordinate, and integrate the implementation of the comprehensive peace process, is committed to continuously uphold the right to privacy of all OPAPP data subjects through the protection of personal data and information as set forth by the provisions of the R.A. 10173 "Data Privacy Act (DPA) of 2012" and its Implementing Rules and Regulations (IRR). All personal

data and information collected through this method of collection, shall be used ONLY for the purpose of the activity. OPAPP shall ensure confidentiality of personal data and information collected through appropriate security measures.

Customized data protection notices and other protocols may be recommended and implemented for other partnerships, programs, projects and activities of the agency.

D. Personal Data and Information Collected and Methods of Collection

OPAPP collects and processes one or more of the following personal data and information based on *Section 3 “Definition of Terms” of the Data Privacy Act of 2012*:

1. **Personal Information** refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual (e.g. *name, office address, office contact number, email address, agency of affiliation, department/office, position*).
2. **Sensitive Personal Information** refers to personal information:
 - a. About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 - b. 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;
 - c. 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
 - d. Specifically established by an executive order or an act of the Philippine Congress to be kept classified.

(e.g. ethnicity, age, sex, gender race, religion, age, political affiliation, marital status, health records, criminal/administrative cases records, social security numbers, licenses, tax returns, occupational and family background information, home address, home contact number, tenure qualifications, firearms records, existing criminal/administrative cases, among others.)

3. **Privileged Information** refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication (e.g. *confidential/secret reports / data / transcripts / manuscripts / letters, meeting proceedings, meeting recordings*)

The collection methods for these types of information include personal data sheets, attendance sheets, registration links, submission of personal and confidential documents, paper and online survey forms, physical and online data and report sharing, among others, and are collected by authorized OPAPP personnel, officers, executives, and legitimate partners.

E. Agency Data Classification, Disclosure, and Authority of Access

The types of personal data and information processed in OPAPP have varying risks that may threaten organizational assets and overall data information and security. All files, records, and documents, in physical and digital format, containing personal data and information are classified in accordance to OPAPP's types of data being processed, and level of accessibility. The data classifications, for records and documents containing personal data and information, found in the Documents and Records Management Procedures were also considered for this categorization.

Table 1. OPAPP Personal Data and Information Classification, and Authority of Access

<i>Personal Data and Information</i>	<i>Applicable Labels⁴</i>	<i>Definition</i>	<i>Authority of Access</i>	<i>Files / Documents / Records Involved</i>
<u>Personal Information</u> <i>e.g. name, office address, contact number, email address, agency of affiliation, department/office, position</i>	<i>Public/Shared/Unclassified/Official</i>	All Records, Files, and Documents, in Physical or Digital format, mandated by law to be publicized, or authorized by the OPAPP officials for release and publication to various dissemination platforms available. Included in this category are records and documents received and generated by	General Public	Program, Project, and Activities (PPA) Progress/Accomplishment and Terminal Reports, Statement of Assets, Liabilities and Net Worth (SALN) (upon request), OPAPP General Directory, Media Coverage Reports <i>Sample OPAPP Documents:</i>

⁴ Top secret – document with information that would cause "exceptionally grave damage" to national security if made publicly available

· Secret - document with information that would cause "serious damage" to national security if it were publicly available

· Confidential - document with information that would cause "damage" or be prejudicial to national security if publicly available

· Restricted – document with information that would cause "undesirable effects" if publicly available

· Official – document with information on the generality of government business, public service delivery and commercial activity

<i>Personal Data and Information</i>	<i>Applicable Labels⁴</i>	<i>Definition</i>	<i>Authority of Access</i>	<i>Files / Documents / Records Involved</i>
		OPAPP , in physical and digital format, tagged according to the Documents and Records Management System Procedures as “ Shared ”, “ Unclassified ” and “ Official ”		Progress Reports of PAMANA, Quarterly Accomplishment Report of OPAPP, Directory of OPAPP officials, Press statements, and OPAPP publications and knowledge products, among others.
<i>Sensitive Confidential</i> <i>e.g. ethnicity, age, sex, gender race, religion, age, political affiliation, marital status, health records, criminal/administrative cases records, social security numbers, licenses, tax returns, occupational and family background information (e.g. names of children, spouse/s, relatives, parents, among others, home address, home phone</i>	<i>Confidential/ Restricted</i>	<p>All Records, Files, and Documents, in Physical or Digital format, that would cause "damage" to the organization or be prejudicial to national security if publicly available, or that would cause “undesirable effects” if publicly available.</p> <p>This may also include all Records, Files, and Documents transmitted/shared to OPAPP and labelled as “Confidential” or “Restricted”, or tagged according to the Documents and Records Management System Procedures as “Restricted” or “Confidential”.</p>	Limited Authorized Contractual and Non-Contractual OPAPP Personnel, Top-level administrators, department heads, deputy heads	<p>Database of peace partners, and actors, OPAPP organized activity resource persons, and participants, building visitors, employee 201 files, Database and profiles of OPAPP’s Program, Project, Activities (PPA) beneficiaries, victims of conflicts (children and adults), Meeting recordings confidential in nature, Database of Former Rebels, Database of Former Violent Extremists, etc.</p> <p><i>Sample OPAPP Documents:</i></p> <p><i>Database of International and Local Peace Partners and</i></p>

<i>Personal Data and Information</i>	<i>Applicable Labels⁴</i>	<i>Definition</i>	<i>Authority of Access</i>	<i>Files / Documents / Records Involved</i>
<i>number, tenure qualifications, firearms records, existing criminal/administrative cases, among others</i>				<i>Donors, HRIS Database, Employee 201 Files, Attendance sheets, visitors' logs, Database of Children and Women victims of Marawi Siege/Sulu bombings, Former Rebel Information System (FRIS), Database of beneficiaries of Programs, Projects, and Activities (PPAs) for Decommissioned Combatants (DCs), MILF & MNLF PDLs, Database of Former CTGs and FVEs applying for E-CLIP, etc.</i>
<u>Privileged Information</u> <i>e.g. secret reports/data/transcripts/manuscripts, meeting proceedings, meeting recordings</i>	<i>Secret/Top Secret</i>	All Records, Files, and Documents, in Physical or Digital format, that would cause "extensive damage" to the organization or cause "exceptionally grave damage" and be prejudicial to national security if publicly available. This may also include all Records, Files, and Documents transmitted/shared to OPAPP labelled as " Secret " or " Top Secret " or tagged according to the Documents and Records Management	Limited Authorized Contractual and Non-Contractual OPAPP Personnel (or Data Privacy Focal Persons), Top-level administrators, department heads, deputy heads	Database of members of Armed Groups, Active Rebels, Legal Case Files, Amnesty Files, Court rulings and proceedings, National Security and Surveillance Reports, etc. <i>Sample Documents:</i> <i>Database of members of Private Armed Groups, National Amnesty Commission (NAC) Files, Amnesty applications to the NAC of 2021,</i>

<i>Personal Data and Information</i>	<i>Applicable Labels⁴</i>	<i>Definition</i>	<i>Authority of Access</i>	<i>Files / Documents / Records Involved</i>
		Procedures as “ Secret ” or “ Top Secret ”.		<i>Recordings of executive sessions of Implementing Panels, Administrative / Legal case files, etc.</i>

Applicable Personal Data and Information Classification Labels must be included in the reports, files, records and documents containing personal data and information processed in physical/paper format. Email subjects for documents containing personal data and information shall likewise indicate agency data classification to control personnel access.

All physical documents for internal release/distribution must be kept in a folder to protect data and information enclosed. Trainings shall be conducted among personnel to ensure awareness on and application of the Personal Data and Information Classification labelling in their daily operations.

F. Internal and External Data and Information Sharing

Personal data and information sharing shall be safeguarded by a standard **Data Request Form** and **Data Sharing Agreement**.

For **External Sharing**, there must be an **official letter of request** from the requesting party supplemented by a **Data Request Form (See Annex B)**. For **Internal (Inter-department) Sharing**, this shall only require a **Data Request Form**. All Data Request Forms shall be processed by the concerned departments and evaluated accordingly and approved by the responsible department’s head. However, the processing, including distribution, of sensitive personal information and privileged information shall be prohibited, except for the cases as provided for in Section 13⁵ of RA 10173 or the Data Privacy Act of 2012 and

⁵ **Section 13. Sensitive Personal Information and Privileged Information.** – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

- (a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;
- (b) The processing of the same is provided for by existing laws and regulations: *Provided, that* such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;
- (c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;
- (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided, that* such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* that consent of the data subject was obtained prior to processing;
- (e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

the provisions set forth by the Memorandum from the Executive Secretary dated 24 November 2016.

All approved **External data request** shall then be governed by the Data Sharing Agreement (*See Annex C: Data Sharing Agreement Template*). Only authorized official/personnel shall be able to co-sign the agreement and share digital or physical data and information to a legitimate and authorized recipient. Personal data and information can only be shared externally once the Data Sharing Agreement is signed by both parties. Upon revocation/termination of the data sharing agreement, all data and information shared must be duly returned to OPAPP or deleted from the other party's database. Likewise, all Memoranda of Agreements shall have a Data Sharing Agreement attachment to ensure that all personal data and information involved and utilized by implementing partners or organizations tapped by OPAPP, are kept confidential and protected. OPAPP shall also request from the other party through the Data Request Forms, a list of all personnel who will gain access to the agency's personal data and information, which shall be one of the basis of the evaluation of the request.

Further, all, except those classified as Public/Shared/Unclassified/Official documents and records containing personal data and information shared electronically, using emails and portable media (e.g. USBs, hard drives), shall at all times be encrypted or password protected. Transmittal of all records, files, and documents containing personal data through facsimile technology is strictly prohibited, while data shared by mail or post shall be transmitted via a registered mail or, where appropriate, guaranteed parcel post service. OPAPP shall also make sure that data shared through these media shall only be delivered to the authorized individual/s.

Meanwhile, pursuant to *Chapter IV, Section 16 "Rights of the Data Subjects"* of the DPA 2012, all external and internal personal data and information requests made by the **owner** of the same can be accessed by the owner himself/herself without the use of a Data Request Form and Data Sharing Agreement. The owner of the personal data and information shall make his or her request through a letter addressed to OPAPP. The concerned department shall process and conduct validation of the said request.

The table below summarizes the Internal and External Data Sharing Requirements.

Table 2. External and Internal Data Sharing Requirements

Type of Request	Requirements
Internal (Within OPAPP, Inter-department)	Approved Data Request Form
External (Outside OPAPP)	Approved Data Request Form, Data Sharing Agreement, and

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority.

	Memorandum of Agreement (MOA), if applicable
External (Outside OPAPP) and Owner of the personal data and information (e.g., amnesty certificate)	Letter addressed to OPAPP

G. Outsourcing and Subcontracting

OPAPP may utilize or outsource the processing of personal data and information by entering into contract with a PIP. The contract shall enumerate the obligations of the PIP including the security measures to be taken to uphold data privacy and their accountabilities should there be violations and/or breaches, and shall be supplemented by a Data Sharing Agreement. All processing activities made by the PIP to personal data and information of OPAPP Data subjects shall also be governed by the rules and regulations under the *DPA IRR Rule X, Section 44 “Agreements for Outsourcing.”*

VI. SECURITY MEASURES⁶

For the past few years of OPAPP’s operation, and its continuous delivery of services to conflict-affected and conflict-vulnerable communities within the country, the agency has put in place data and information security measures to protect its organizational assets and protect its stakeholders’ right to privacy. The following measures shall be strictly adhered to by all OPAPP personnel and management in processing personal data:

A. Organizational Measures

As a Personal Information Controller (PIC), OPAPP must effectively implement the following measures in the efforts to safeguard the human aspect of data protection:

1. Privacy Impact Assessment (PIA)

OPAPP shall conduct an annual departmental and organizational privacy impact assessment to assess the integrity of all its personal data and information security measures relative to its mandates, functions, programs, projects, activities and systems. The two-step privacy impact assessment shall adhere to the following process:

⁶ R.A. 10173, IRR, Rule No. 6, “Security Measures for Protection of Personal Data”

Table 3. OPAPP PIA Process and Timeline

Activity	Facilitating Department/s/ Teams / Focal	Description	Proposed Timeline
Departmental / Area Management Office PIA	Policy and Strategic Planning Department (Data Privacy Mechanism), Department/Area Management Privacy Focal (DPF)	The PIA shall start with a departmental assessment facilitated by the designated Department Privacy Focal (DPF), using the National Privacy Commission toolkit. The said activity shall take place two (2) weeks before the conduct of the overall privacy impact assessment. Further, this activity shall result in the documentation of the departments’/AMOs’ inventory of PPAs involving the processing of personal data and information, privacy risks assessments, identification of privacy threats, and formulation of recommendations to address identified gaps. This activity may also be included in the respective departments’ planning and assessment schedules.	4 th Quarter of every year

Activity	Facilitating Department/s/ Teams / Focal	Description	Proposed Timeline
Organizational PIA	Composite Team (CT) - ICTD; PSPD; MEALD; Administrative Department-Records Management Unit/ Archives; HRMD; and, KMPID	The departmental / area management office PIA results shall be consolidated to be presented during the organizational PIA. This activity shall be a platform to gather additional inputs and insights on data privacy and develop recommendations for the improvement of the systems and measures in place, as well as, for the enhancement of this Manual.	

The **Organizational PIA** shall also include a session dedicated for the **Privacy Planning** to identify necessary security risks to be implemented based on the PIA immediate findings from the Department PIA, and a **Privacy Manual Review and Updating**.

2. Designation of Data Protection Officer (DPO), and Alternate

A DPO for OPAPP and his or her alternate shall be designated through an issuance of an office order. The DPO and his or her alternate shall have the ranks of Undersecretary and Director, respectively.

The following are the functions of the DPO and/ or his or her alternate as prescribed by the NPC:

- a. Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:
 - i. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
 - ii. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;

- iii. Inform, advise, and issue recommendations to the PIC or PIP relative to data protection;
 - iv. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and,
 - v. Advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law.
- b. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
 - c. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
 - d. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
 - e. Inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and issuances of the NPC;
 - f. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
 - g. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns and the PIC or PIP;
 - h. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
 - i. Perform other duties and tasks that may be assigned by the head of the PIC that will ensure data privacy and security and uphold the rights of the data subjects.

3. Establishment of a Composite Team

The agency shall establish a composite team to assist the DPO and his or her alternate in performing their duties. The following are the departments whose representatives shall compose the team (Junior or Senior Technical Staff).

- a. Information and Communications Technology Division (ICTD);
- b. Policy and Strategic Planning Department (PSPD);
- c. Monitoring, Evaluation, Accountability and Learning Department (MEALD);

- d. Administrative Department-Records Management Unit/ Archives
- e. Human Resource Management Department (HRMD); and,
- f. Knowledge Management and Peace Institute Department (KMPID).

The following are the functions of the Composite Team:

- a. Assist in the monitoring of the agency's compliance to the DPA;
- b. Facilitate the conduct of Privacy Impact Assessments with the Policy and Strategic Planning Department;
- c. Assist in the agency's compliance of DPA pillars;
- d. Coordinate with the Breach Response Team in case there are complaints received on data breaches; and;
- e. Perform other duties and tasks as maybe assigned by the DPO in relation to data protection and security.

The designation of the Composite Team shall be made official through an office order.

4. Designation of Department/Area Management Privacy Focal Persons (DPF)

OPAPP departments and Area Management Offices (AMO) shall nominate a DPF, which can be a junior/senior technical staff, tasked to represent the department in the privacy-related activities. Designated individuals shall also join the DPO, CT, and the Breach Response Team (BRT) in the trainings, seminars, and workshops related to the DPA, as well as participate in the formulation of policies and measures to ensure data and information security within the agency. The DFP shall also be responsible in ensuring adherence to privacy measures, monitoring and reporting security incidents, such as data breach and privacy concerns, within their departments and AMOs. The designation of the DPFs shall be made official through an office order. The fulfillment of their roles and responsibilities shall be accounted for in their Individual Performance Commitment Report (IPCR).

5. Non-Disclosure Agreement (NDA) Requirement for all Employees, Service Providers and Technical Consultants

All employees, both contractual and non-contractual from both OPAPP central office and the area management offices shall be required to sign a *Non-Disclosure Agreement (NDA) for Employees (Annex D)*. All personnel processing personal data and information shall strictly keep all records and files, both physical and digital, confidential, even after retiring and resignation. All service providers and technical consultants who shall collect and process personal data and information shall likewise sign a *NDA (Annex DI)* to be attached to their contract.

6. Data Privacy and Information Security Capacity Development Trainings and Seminars

To continuously build and develop capacity and enhance knowledge of OPAPP personnel in the measures to effectively protect personal data and information within their respective offices and protect the agency from potential losses due to data breach, the following are the trainings recommended:

Table 4. Proposed Trainings and Seminars and Target Beneficiaries

Trainings	Target Beneficiaries
Privacy Manual Cascading	Composite Team, DPF, OPAPP Department technical and administrative personnel
Training on the use of the NPC Toolkit for the Conduct of Department Privacy Impact Assessments	DPFs
Data Information and Cybersecurity Learning Sessions	Representatives from various OPAPP departments and Area Management Offices, DPF
Physical Data and Information Handling	OPAPP messengers, and motor pool members, utility personnel, handling and delivering physical files containing personal data and information.
Data Classification and Labelling and Records and Document Management	Human Resource Management Department (HRMD), Finance Department, Information and Communications Technology Division (ICTD), Personnel Performing Technical and Administrative work involving personal data and information, including utility workers, among others.
Breach Response Training	Breach Response and Composite Teams, and DPF
Orientation on the Data Privacy Act	All OPAPP personnel (contractual and non-contractual)
Orientation on Citizen's Charter	All OPAPP personnel (contractual and non-contractual), especially the newly-hired employees.

These recommended trainings may be updated regularly based on the need.

7. OPAPP Activity Documentation and Recording

The respective departments of OPAPP and the DPO shall maintain accurate documentation and recording of all relevant activities, systems, and processes. These documentations and recordings must be kept on file in a safe and secure repository for privacy risk assessments to be done annually, and for all applicable privacy registration processes. Consents for media coverage, interviews, research purposes, and photo-documentations, must at all times be secured to avoid legal repercussions. Assent forms coupled with Parental Consent forms shall be accomplished when conducting OPAPP related programs/projects/activities that involve children (*Younger than 18 years old*). All consent and assent forms shall also be translated in the local language. (*See Annex E, E1, E2: Consent, Parental Consent and Assent Forms Template*)

8. DPA Compliance Internal Audit and Assurance

To ensure that OPAPP's policies and measures are compliant to the DPA, the agency shall also undertake an internal audit and assurance program through annual internal compliance monitoring, and when necessary, outsource privacy compliance auditors. The agency shall also prepare for NPC-initiated compliance and privacy sweeps, as well as onsite visits.

B. Physical Measures

The protection of OPAPP's office perimeters, equipment and local networks, shall be protected from physical breach and avoid organizational losses. Office equipment, storage facilities and other areas of the office building must be kept safe from mechanical destruction, network and wire-tapping, and trespassing. The following provisions are hereby being included in this Manual for adherence.

1. Data Format, Storage Type, Location, Retention, and Disposal

All personal data and information collected by OPAPP maybe in the form of digital/electronic or physical/paper-based format. All files, physical or digital must be kept safe from potential threats such as data breach, and unauthorized use and disclosure. The following measures must be followed when storing, retaining and disposing personal data and information:

Table 5. Data and Information Management Measures

Personal Data and Information Format	Storage Type/s	Storage Location	Retention	Disposal Measure
Physical / Paper-based	Filing cabinets, water-proof, file folders,	Designated office areas/room, within	As stipulated in <i>Section 19 of DPA IRR</i> , Personal data and information shall	All files under this classification must be disposed

Personal Data and Information Format	Storage Type/s	Storage Location	Retention	Disposal Measure
	binders, file cases, laterals, etc.	OPAPP premises	be kept as long as necessary and/or as prescribed by R.A. 9470 or the National Archives of the Philippines (NAP) Act of 2007 (<i>See Annex F for the NAP Circular 2: Prescribed retention periods for each specific record</i>), and other related policies, unless otherwise instructed by the department head, officer or executive. It shall likewise abide by the regulations	properly once authorized or have reached the prescribed retention time. This shall follow the established Records and Documents Management Procedures prescribed methods of disposition such as shredding, and incineration, among others.
Digital / Electronic	Cloud, OPAPP servers, office computers, and storage devices, etc.	Within OPAPP network, within OPAPP premises	set forth by OPAPP's Documents and Records Management Control Procedures.	All files under this classification must be deleted from the OPAPP's cloud storage, storage devices, and networks, once authorized or have reached the prescribed retention time, and shall follow the established

Personal Data and Information Format	Storage Type/s	Storage Location	Retention	Disposal Measure
				Records and Documents Management Procedures prescribed methods of disposition such as device formatting, remote deletion.

Personal data and information, received in the physical / paper-based format must be kept in a designated room/area within the respective departments and AMOs. It shall likewise be digitized through scanning for back-up, and must be stored in authorized storage facilities for digital / electronic data. Labels of personal data and information shall be properly indicated using the data classification and labels found in **Table 2, and all data classification labels set forth by the Records and Documents Management Procedures and Policies, as well as the provisions of R.A. 9470 or the National Archives of the Philippines Act of 2007 and its Implementing Rules and Regulations (IRR).**

Personal data and information of OPAPP personnel (e.g., Personal Data Sheet, SALN, Contracts, etc.) shall be secured and not be exposed in plain view. Concerned departments and personnel shall ensure these are not exposed to others in the office premises except to the authorized personnel.

2. Access Procedure of Agency Personnel

Departments and area management offices must designate personnel authorized to access the filing cabinets/storage areas/rooms, files of personal data and information. A list of designated personnel must be submitted by the DPF to the DPO through the composite team for access monitoring.

3. Monitoring and limitation of access to file storage room or facility

All file cabinets, file storage rooms/areas, holding personal data and information files and records within each department and AMOs, must have a log book to monitor access to the said areas. Log books must record the following details:

- a. Date and Time of Access
- b. Name of Personnel

- c. Physical File number / code accessed / taken
- d. Purpose
- e. Date and Time returned for files taken

Log books must be monitored regularly by the designated authorized personnel for monitoring. Physical files taken out of the room/file cabinet must be authorized and cleared by the designated personnel, and must be returned immediately. It is also prohibited for unauthorized personnel to keep official copies of documents containing personal data and information. Bringing of devices which have the capacity to take photos are prohibited in accessing the file storage rooms.

4. Clean Work Station Policy

Work stations in the offices, including computer monitors, must be cleared during break times and end of work day to avoid breach of privacy. Work files containing personal data and information must not be exposed in plain view for protection. All devices and equipment used for personal data and information processing must be password protected.

5. Field Work Station Protocols

All personnel on official field work and travel shall ensure that no unauthorized person can view or manipulate files and reports containing personal data and information. Computers must be closed or turned off when leaving the equipment in a specific area. All devices and equipment used for personal data and information processing must be password protected. Physical files must be stored in secured and labeled container to avoid unauthorized viewing.

6. Equipment Inventory and Check Ups

Each department and AMO, through designated personnel and in collaboration with the DPF, must conduct annual inventory of equipment and devices used for personal data and information processing (e.g. computers, printers, hard drives, copying machines, etc.), in accordance to *Section 490, "Physical Stock-Taking" of the Government Accounting and Auditing Manual (GAAM)* of the Commission on Audit (COA). The inventory list must be included in the Department and Area Management Office PIA to be submitted to the Composite Team for the overall PIA presentation during the organizational PIA.

7. Office Work Space Design

Work stations in the offices must be designed to ensure privacy. Computer screens must not face the entrance of the office to avoid unauthorized persons/guest to view files/details of working files. Ample spaces between each work stations must also be maintained.

8. Perimeter Security

The OPAPP building, containing personal data and information files and reports, must be protected from trespassing and unauthorized access to prevent data loss and security breach. The whole office perimeter must have security cameras recording 24/7, with its footages backed-up and secured regularly. Entrances for official guests, suppliers, and couriers, among others, must be guarded by security personnel equipped with logbooks and visitor/delivery badges.

C. Technical Measures

OPAPP, being a PIC, must lay down technical security measures to ensure that personal data and information and processing are protected from imminent danger. These include the protection of computer networks, establishment of encryption mechanisms, among others to control and limit access. The following are the measures to be adopted:

1. Monitoring of Security Breaches

The organization shall use a firewall to capture ingress or egress vulnerabilities to monitor security breaches and alert the organization of any attempt to interrupt or disturb the system and networks. All systems in place must be updated to adapt to the present need and availability of technology. All security breaches must be documented and responded by the breach response team, in coordination with the DPO, Composite Team, and DPF.

2. Security features of the software/s and application/s used

OPAPP, shall ensure that software installation to all agency-owned equipment and devices are limited. All software and applications to be installed must be evaluated by the ICTD before installation. OPAPP shall ensure that anti-virus applications are installed in all computers and shall be regularly updated.

3. Process for regular testing, assessment and evaluation of effectiveness of security measures

Regular assessment of data and information security measures being implemented by the agency shall be evaluated annually through the PIA to ensure integrity and reliability.

4. Email Protocol and Encryption

External sharing and disclosure of documents and files containing personal data and information must only be done by authorized personnel and coursed through official OPAPP emails. Files must be password protected using the data encryption tools available. Passwords of encrypted files may be shared to the authorized recipient through encrypted messaging applications or in a separate email. Official personnel emails must contain a

notification stating that the email recipient is the only authorized person to view the files involved.

VII. BREACH AND SECURITY INCIDENTS⁷

This section enumerates the measures and protocols in addressing breach and security incidents within the agency. The following are the provisions under this section:

A. Creation of a Data Breach Response Team (BRT)

The **Breach Response Team** shall monitor and respond to all breach and security incidents within the agency. The team shall be led by the **Information and Communications Technology Division (ICTD)** and shall be composed of representatives (junior/senior technical staff) from the following Departments:

- a. Policy and Strategic Planning Department (PSPD)
- b. Legal Affairs Department (LAD)
- c. Communication and Public Affairs Department (CPAD)
- d. Information and Communications Technology Department (ICTD)

The following are the functions of BRT:

- a. In coordination with the DPO, ensure the implementation of the security incident management policy of the PIC and contracted personal information processor;
- b. Manage security incidents and personal data breaches;
- c. Assess and evaluate a security incident, restore integrity to the information and communications system, mitigate and remedy any resulting damage;
- d. Prepare documentation reports on data breaches and actions taken by the PIC to address the same and submit to the DPO for submission to NPC; and,
- e. Ensure compliance by the PIC and its contracted PIP with the relevant provisions of the Act, its IRR, and all related issuances by the Commission on personal data breach management.

The designation of the breach response team shall be made official through an office order.

B. Measures to prevent and minimize occurrence of breach and security incidents

Apart from the regular conduct of the PIA and Privacy Policy Review and Updating, the Composite Team in collaboration with the BRT and the DPFs, shall also implement additional measures to prevent breach and security incidents. This shall include regular perimeter check-ups, network scanning, and provision of trainings to the personnel directly involved in the processing

⁷ R.A. 10173, IRR, Rule No. 9, "Data Breach Notification", NPC Circular 16-03 – Personal Data Breach Management

of personal data and information. Regular **breach response drills** participated in by the DPF and the Breach Response Team, shall be conducted semi-annually to better prepare the agency in responding to breach and security incidents.

C. Back Up and Restoration of Personal Data and Information

All files in custody containing personal data and information must be backed-up through digitization and scanning to prevent data loss and stored in secured storage facilities. This must be ensured by designated DPF. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

D. Breach and Security Incident Evaluation, Reporting, and Notification Protocol

In case of a breach or security incident, OPAPP shall follow a standard Privacy Security Incidents and Breaches Reporting and Security Incident Management Flow.

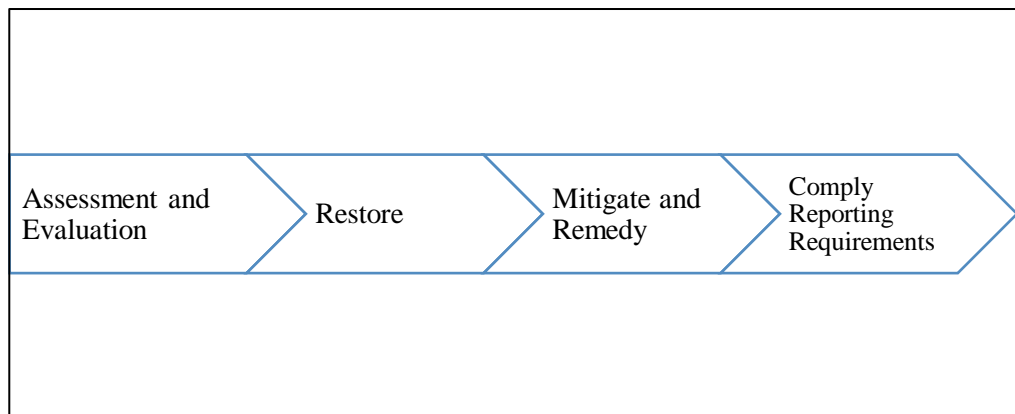


Figure 1. Security Incident Management Flow

The BRT, in coordination with all relevant DPFs, shall assess and evaluate every security breach incident. The team shall at all times prioritize the restoration of all process affected by the incident, as well as the mitigation and fixing all incurred damages.

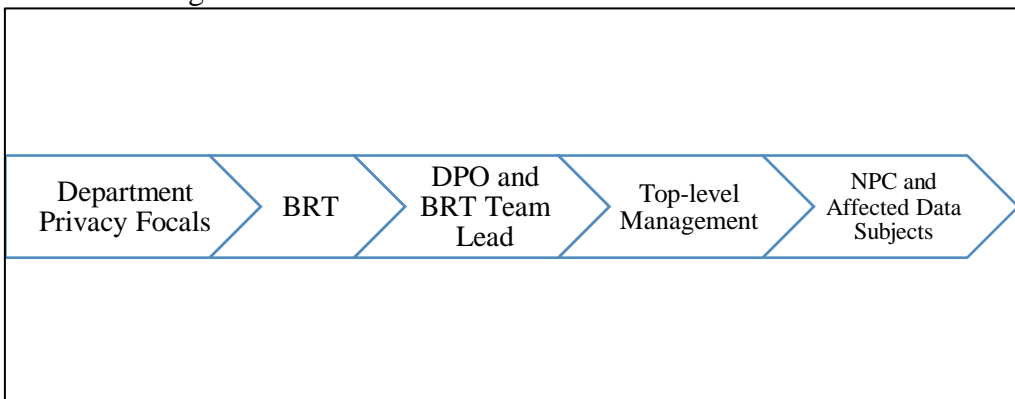


Figure 2. Privacy Security Incidents and Breaches Reporting Structure

Processing of privacy security breaches begins with an incident report from all involved departments, the incident report shall be handled by the BRT following a standard breach response protocol. Outcomes shall then be reported to appropriate top-level managers, the NPC, and the affected OPAPP data subjects. Documentation shall at all times be secured in all related compliance and incident matters using the NPC prescribed templates.

E. Data Breach and Security Breach Documentation Protocol

Using the Privacy and Security Incidents and Breaches Reporting Structure, the Breach Response Team, in collaboration with the concerned Department/Area Management Privacy Focal (DPF) shall prepare a detailed documentation of every security incident or breach encountered, including an annual security incident report to be submitted to the management and the NPC (*See Annexes G and G1 for the NPC Prescribed Annual Security Incident Report Template and Mandatory Security Incident Notification Template*). All relevant OPAPP data subjects must be notified within seventy-two (72) hours upon knowledge of or reasonable belief by the agency that a personal data breach has occurred (**See Annex G2 for the Mandatory Notification Template for Data Subjects**).

VIII. INQUIRIES AND COMPLAINTS

All OPAPP data subjects have the right to access the Privacy Manual and all relevant documents and policies for the protection of personal data and information. They shall be given platforms to exercise the following rights: (1) right to dispute the inaccuracy or error in the personal data; (2) right to request the suspension, withdrawal, blocking, removal or destruction of personal data; and (3) right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data.

In furtherance of the DPA, and in complementation to the purposes of the *Executive Order No. 2, s. 2016 "Freedom of Information (FOI) Law"*, OPAPP Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the agency, including the data privacy and security policies implemented to ensure the protection of their personal data. They may write to the organization at **opapp.foi@gmail.com** and briefly discuss the inquiry, together with their contact details for reference.

Feedback and complaints regarding Data Privacy may be coursed through the OPAPP Feedback Response System (FRS) through **<https://frs.peace.gov.ph>** or **peace.monitoringandevaluation@gmail.com**. The concerned departments or units shall confirm with the complainant its receipt of the complaint and the status and actions taken in response thereto.

IX. ANNEXES

LIST OF ANNEXES

ANNEX A	OPAPP Data Privacy Notice
ANNEX B	Data Request Form Template
ANNEX C	Data Sharing Agreement Template
ANNEX D	Non-Disclosure Agreement Template for Employees
ANNEX D1	Non-Disclosure Agreement Template for Consultants
ANNEX E	Consent Form Template
ANNEX E1	Assent Form Template
ANNEX E2	Parental/Legal Guardian Consent Form Template
ANNEX F	NAP: General Records Disposition Schedule
ANNEX G	Annual Security Incident Reports for PICs Template
ANNEX G1	Mandatory Notification Template: Personal Data Breach for the National Privacy Commission
ANNEX G2	Mandatory Personal Data Breach Notification for Data Subjects

ANNEX A

OPAPP DATA PRIVACY NOTICE

The Office of the Presidential Adviser on the Peace Process (OPAPP), mandated to oversee, coordinate, and integrate the implementation of the comprehensive peace process, is committed to continuously uphold the right to privacy of all OPAPP data subjects through the protection of personal data and information as set forth by the provisions of the R.A. 10173 Data Privacy Act of 2012 (DPA) and its Implementing Rules and Regulations.

This notice generally elaborates the purpose and legal basis for the processing of personal data and information collected from OPAPP data subjects. This document shall also explain the security measures being adopted by the agency to protect the fundamental right to privacy, and effectively implement programs, projects, and activities in accordance to its mandates.

OPAPP SERVICES

In accordance to its mandates, OPAPP generally provides interventions and carries out functions to achieve the Six (6) Paths to Peace:

1. Pursuit of Social, Economic and Political Reforms- involves the vigorous implementation of various policies, reforms, programs and projects aimed at addressing the root causes of internal armed conflicts and social unrest. This may require administrative action, new legislation or even constitutional amendments.
2. Consensus-Building and Empowerment for Peace- includes continuing consultations on both national and local levels to build consensus for a peace agenda and process, and the mobilization and facilitation of people's participation in the peace process.
3. Peaceful Negotiated Settlement with Different Rebel Groups- involves the conduct of face-to-face negotiations to reach peaceful settlement with the different rebel groups. It also involves the effective implementation of peace agreements.
4. Programs for Reconciliation, Reintegration into Mainstream Society and Rehabilitation- includes programs to address the legal status and security of former rebels, as well as community-based assistance programs to address the economic, social and psychological rehabilitation needs of former rebels, demobilized combatants and civilian victims of the internal armed conflicts.
5. Addressing Concerns Arising from Continuing Armed Hostilities- involves the strict implementation of laws and policy guidelines, and the institution of programs to ensure the protection of non-combatants and reduce the impact of the armed conflict on communities found in conflict areas.
6. Building and Nurturing a Climate Conducive to Peace- includes peace advocacy and peace education programs, and the implementation of various confidence-building measures.

PERSONAL INFORMATION COLLECTED AND METHODS OF COLLECTION

OPAPP collects and processes one or more of the following personal data and information based on the provision of the Data Privacy Act of 2012:

1. Personal Information such as name, sex, gender, address, contact number, email address, agency of affiliation, department/office, position, name of relatives/siblings/spouse/children;

2. Sensitive Personal Information such as ethnicity, age, political affiliation, marital status, health records, criminal/administrative cases records, social security numbers, licenses, tax returns, occupational background, tenure qualifications, firearms records, criminal/administrative cases; and
3. Privileged Information such as confidential/secret reports/data/transcripts/manuscripts, meeting proceedings, meeting recordings.

The collection methods for these types of information include personal data sheets, submission of personal and confidential documents, paper and online survey forms, physical and online data and report sharing, among others, and are collected by OPAPP authorized OPAPP personnel, officers, executives, and legitimate partners.

PURPOSES OF PROCESSING PERSONAL DATA AND INFORMATION

OPAPP processes personal data and information using one or more of the following grounds:

1. Performance of the agency's obligations and deliverables in accordance to its mandates as a national government agency pursuant to Executive Order 125, series of 1993, as amended by Executive Order 3, series of 2001.
2. Protection of privacy rights and welfare of OPAPP Data Subjects in accordance to the RA 10173 or the Data Privacy Act of 2012 and other policy issuances of the NPC.
3. Overall internal and external operational management as a national government agency and Personal Information Controller.

In accordance to the abovementioned, OPAPP processes personal data and information for the following purposes:

1. Delivery of services to conflict-affected and conflict-vulnerable areas through the agency's programs, projects, and activities;
2. Overall operational management of OPAPP departments and area management offices, including administrative and technical operations, among others;
3. Management of human resources, including external sources of technical service providers and prospective human resources;
4. OPAPP data subjects external and internal affairs and relations;
5. Database and Records keeping and maintenance,
6. Documentations;
7. Media Coverage;
8. Corporate and governance requirements and due diligence;
9. Partnerships, donors' management, and external relations; and
10. Any other activities that may deem processing personal data and information relevant and necessary.

OPAPP Data Subjects shall be notified for appropriate consent should their personal data and information in the agency's custody are to be used aside from the above mentioned circumstances.

TIMING OF COLLECTION

Personal data and information are collected as needed in accordance to OPAPP's mandates, with the OPAPP Data Subjects' consent, in the effective implementation of the agency's programs, projects and activities.

STORAGE, TRANSMISSION, RETENTION, AND DISPOSAL OF PERSONAL DATA AND INFORMATION

All files, physical or digital are kept safe from potential threats such as data breach, and unauthorized use and disclosure. The following measures are followed when storing personal data and information:

Personal Data and Information Format	Storage Type/s	Storage Location	Retention	Disposal Measure
Physical / Paper-based	Filing cabinets, water-proof, file folders, binders, file cases, laterals, etc.	Designated office areas/room, within OPAPP premises	As stipulated in <i>Section 19 of DPA IRR</i> , Personal data and information shall be kept as long as necessary and/or as prescribed by R.A. 9470 or the National Archives of the Philippines (NAP) Act of 2007 (<i>See Annex F for the NAP Circular 2: Prescribed retention periods for each specific record</i>), and other related policies, unless otherwise instructed by the department head, officer or executive. It shall likewise abide by the regulations set forth by OPAPP's Documents and Records Management Control Procedures.	All files under this classification must be disposed properly once authorized or have reached the prescribed retention time. This shall follow the established Records and Documents Management Procedures prescribed methods of disposition such as shredding, and incineration, among others.
Digital / Electronic	Cloud, OPAPP servers, office computers, and storage devices, etc.	Within OPAPP network, within OPAPP premises		All files under this classification must be deleted from the OPAPP's cloud storage, storage devices, and networks, once authorized or have reached the prescribed retention time, and

				shall follow the established Records and Documents Management Procedures prescribed methods of disposition such as device formatting, remote deletion.
--	--	--	--	--

Personal data and information, received in the physical/paper-based format are digitized through scanning for back up, and are stored in authorized storage facilities for digital/electronic data. Confidential and sensitive personal data and information are to be properly labelled according to the classification set by OPAPP in its Privacy Manual, and secured in a cabinet.

Moreover, all personal data and information sharing shall be safeguarded with standard safety measure including password protection/and or encryption for digital files and appropriate labelling of physical files. Disclosure of personal data and information outside OPAPP shall be accompanied with appropriate data sharing agreements.

RIGHTS OF OPAPP DATA SUBJECTS

Pursuant to the RA 10173 Data Privacy Act of 2012 and its Implementing Rules and Regulations, all OPAPP Data Subjects are entitled to the following rights.

1. Be informed on whether your personal information shall be, are being or have been processed;
2. Be furnished with the information indicated below before the entry of your personal information into the processing system of the Personal Information Controller, or at the next practical opportunity:
 - a. Description of the personal information to be entered into the system;
 - b. Purposes for which they are being or are to be processed;
 - c. Scope and method of the personal information processing;
 - d. The recipients or classes of recipients to whom they are or may be disclosed;
 - e. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
 - f. The identity and contact details of the personal information controller or its representative;
 - g. The period for which the information will be stored; and
 - h. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.
3. Any information supplied or declaration made to you on these matters shall not be amended without prior notification: Provided, That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee

relationship, or when the information is being collected and processed as a result of legal obligation;

4. Reasonable access to, upon demand, the following:
 - a. Contents of your personal information that were processed;
 - b. Sources from which personal information were obtained;
 - c. Names and addresses of recipients of the personal information;
 - d. Manner by which such data were processed;
 - e. Reasons for the disclosure of the personal information to recipients;
 - f. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect you;
 - g. Date when your personal information was last accessed and modified; and
 - h. The designation, or name or identity and address of the personal information controller.
5. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, that the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon your request;
6. Suspend, withdraw or order the blocking, removal or destruction of your personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information is incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected; and,
7. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.
8. Right to data portability - where personal information is processed by electronic means and in a structured and commonly used format, you have the right to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use.

INQUIRY

In furtherance of the DPA, and in complementation to the purposes of the FOI law, OPAPP data subjects may inquire or request for information regarding any matter relating to the processing of personal data and information through opapp.foi@gmail.com. Feedback and complaints regarding Data Privacy may also be coursed through the OPAPP Feedback Response System (FRS) through <https://frs.peace.gov.ph> or peace.monitoringandevaluation@gmail.com.

ANNEX B
DATA REQUEST FORM

Requesting Party (“Personal Information Requester”) <i>(Name of Agency, Organization, Entity)</i>	
Office Address:	
Office Number/s:	
Office E-mail Address:	
Contact Person <i>Name</i> <i>Position</i> <i>Department/Division/Unit</i> <i>Contact Number</i> <i>Email address</i>	
Data/Information Requested: (Indicate which data from <u>Department/Area Management Office</u> being requested, include inclusive dates, focus area, etc.)	
Data Format (Tick appropriate box)	<input type="checkbox"/> PDF <input type="checkbox"/> Excel <input type="checkbox"/> Word <input type="checkbox"/> Physical Others: _____
Purpose of Data and Information Requested (Indicate nature of program/project/activity the data and information are being used in, inclusive dates)	
List of Personnel who will gain Data and Information Access <i>Name/s</i> <i>Position/s</i> <i>Department/s/Division/s/Unit/s</i> <i>Contact Number/s</i> <i>Email address/s</i>	
The Requesting Party agrees that OPAPP shall have the perpetual, irrevocable and unconditional right to request for the results / outcomes of the program / project / activity in which the data requested was used, and to use, publish, copy and disseminate such results and outcomes in	<input type="checkbox"/> Yes <input type="checkbox"/> No

Please attach to the official letter of data request.

any form, for any purpose and in any manner whatsoever. To this end, the Requesting Party will provide OPAPP with a copy of the results in a computer readable format. Further, if this request is approved, the Requesting Party shall also adhere to the provisions stipulated in the Data Sharing Agreement and the provisions set forth by the Data Privacy Act of 2012.

(Tick appropriate box)

NAME AND SIGNATURE OF AUTHORIZED REPRESENTATIVE
Requesting Party

This portion shall be processed and signed by the concerned OPAPP representatives.

RECEIVED AND PROCESSED BY:

NAME AND SIGNATURE OF OPAPP DEPARTMENT PERSONNEL
NAME OF OPAPP DEPARTMENT

APPROVED/DISAPPROVED BY:

NAME AND SIGNATURE OF DEPARTMENT HEAD
NAME OF OPAPP DEPARTMENT

Please attach to the official letter of data request.

ANNEX C¹

DATA SHARING AGREEMENT

KNOW ALL MEN BY THESE PRESENTS:

This **DATA SHARING AGREEMENT** (the “Agreement”) is made and entered into on _____ in _____ by and between:

OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS (OPAPP) a government agency duly organized and existing under the laws of the Republic of the Philippines, with principal place of business at Agustin 1 Building, Ruby Road., Barangay San Antonio, Ortigas Center, Pasig City, represented hereinafter referred to as the “**PERSONAL INFORMATION CONTROLLER**” and represented by our **AUTHORIZED OFFICIAL/PERSONNEL**, _____ (name) _____.

And

MR/MS. _____, Filipino Citizen, married/single and of legal age with residence at _____ and hereinafter referred to as the “**PERSONAL INFORMATION REQUESTER**” (together, the “**PARTIES**”);

WITNESSETH: That

WHEREAS, the **PARTIES** have entered into a Memorandum of Agreement on _____ in _____.

WHEREAS, in order to give full force and effect to the provisions of the Memorandum of Agreement, the **PERSONAL INFORMATION CONTROLLER** is required to disclose and/or transfer to **PERSONAL INFORMATION REQUESTER** certain personal data under the custody of the **PERSONAL INFORMATION CONTROLLER**.

WHEREAS, under Section 20(b)(2) of the Implementing Rules and Regulations of Republic Act No. 10173, data sharing for involving government agencies and non-government agencies shall be covered by a data sharing agreement.

NOW THEREFORE, for and in consideration of the foregoing premises, and for purposes of complying with the provisions of the Data Privacy Act of 2012, the **PARTIES** hereby agree and bind themselves as follows:

1. DEFINITION OF TERMS: As used herein, the following terms shall have the respective meanings hereafter set forth:

- a. “Data sharing” shall mean the disclosure or transfer to a third party of personal information under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.
- b. “Data Subject/s” shall mean an individual/s whose personal information is processed.
- c. “Personal information” shall mean 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.

¹NPC Toolkit

- d. “Privileged information” shall mean any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.
 - e. “Processing” refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
2. **EFFECTIVITY:** This Agreement shall have full force and effect upon transmittal of the PERSONAL INFORMATION CONTROLLER of any type of personal information in relation to the Data Subject acquired pursuant to the implementation of the Memorandum of Agreement.
 3. **DISCLOSURE:** Notwithstanding the provision of the previous paragraph, the PERSONAL INFORMATION CONTROLLER, shall disclose to the Data Subject/s the following information prior to the collection and sharing of personal data to PERSONAL INFORMATION REQUESTER:
 - a. Identity of the PERSONAL INFORMATION CONTROLLER and the PERSONAL INFORMATION REQUESTER, if any, that will be given access to the personal information;
 - b. Purpose of data sharing;
 - c. Categories of personal information concerned;
 - d. Intended recipients or categories of recipients of the personal information;
 - e. Existence of the rights of Data Subject/s, including the right to access and correction, and the right to object; and,
 - f. Other information that would sufficiently notify the Data Subject/s of the nature and extent of data sharing and the manner of processing.
 4. **CONSENT:** The PERSONAL INFORMATION CONTROLLER shall obtain the consent of the Data Subject/s to the data sharing between the PARTIES.
 5. **GENERAL DATA PRIVACY AND DATA SHARING PRINCIPLES:** The PARTIES adopt the general data privacy and data sharing principles declared in the Data Privacy Act of 2012 and its Implementing Rules and Regulations, and adhere to the principles of transparency, legitimate purpose, and proportionality in the processing of personal data under this Agreement.
 6. **SAFEGUARDS FOR DATA PRIVACY AND SECURITY:** The PARTIES shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data that are subject to data sharing.

The PARTIES shall take appropriate steps to ensure that any person acting under their authority and who has access to personal data does not process them except only for the purpose agreed upon by the PARTIES and to give effect to the Memorandum of Agreement/Contract as required by law.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any natural dangers such as accidental loss or unlawful destruction, and human dangers such as alteration and contamination, disclosure, unlawful access and processing, fraudulent misuse, unlawful destruction.

The Personal Information requester shall provide OPAPP with a copy of the results in a computer readable format.

The PARTIES shall ensure that the said measures will enable them to comply with the guidelines for organizational, physical, and technical security measures, as provided in the Data Privacy Act of 2012, and its Implementing Rules and Regulations.

7. **TERMINATION:** This agreement may be terminated upon the expiration of its term, or any valid extension thereof; upon the agreement by all parties; upon a breach of its provisions by any of the

parties; or where there is disagreement, upon a finding by the Commission that its continued operation is no longer necessary, or is contrary to public interest or public policy. All personal data transferred to the PERSONAL INFORMATION REQUESTER by virtue of this agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement.

8. **GOVERNING LAW:** This Agreement is governed by the laws and policies of the Philippines.
9. **DISPUTE SETTLEMENT:** Should it be necessary that an action be brought to enforce any of the terms of this Agreement, the same should be brought in the proper courts of _____ only, to the exclusion of all other courts.

IN WITNESS WHEREOF, the PARTIES hereto have set their hands on the date and in the place first above written.

OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS	PERSONAL INFORMATION REQUESTER
NAME OF THE HEAD OF THE AGENCY/AUTHORIZED OFFICIAL/PERSONNEL	NAME OF REPRESENTATIVE
Secretary	Position

WITNESSED BY:

ACKNOWLEDGMENT

Republic of the Philippines)
) S.S.

BEFORE ME, this _____ in _____, personally appeared the following:

NAME	GOVERNMENT ISSUED ID

who were identified by me through their competent evidence of identity to be the same persons who executed the foregoing document. Further, the parties acknowledged to me that the same is their true and voluntary act and deed, and the true and voluntary act and deed of the entities they represent, after the same document has been interpreted to them by me in a language and dialect known to them.

IN WITNESS WHEREOF, I have hereunto signed and affixed my notarial seal in the place and on the date first above written.

Doc. No. ____;
Page No. ____;
Book No. ____;
Series of ____;

ANNEX D
NON-DISCLOSURE AGREEMENT TEMPLATE FOR EMPLOYEES

Office of the President of the Philippines
OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS

NON-DISCLOSURE AGREEMENT

The **OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS**, herein referred to as “OPAPP”, the undersigned employee hereby agrees and acknowledges:

1. That during the course of my employ there may be disclosed to me certain information from OPAPP; said information consisting of but not limited to:
 - a. Technical information: methods, processes, frameworks, compositions, research projects and publications.
 - b. Classified information: technical data in the possession of OPAPP that are considered as classified and/or confidential due to its implications on national security consisting of but not limited to data concerning the different Peace Processes of the Philippine Government.
2. I agree that I shall not during, or at any time after the termination of my employment with OPAPP, use for myself, or disclose or divulge to others including future employees, any trade secrets, confidential information, or any other proprietary data of OPAPP in violation of this agreement.
3. That upon the termination of my employment from OPAPP:
 - a. I shall return to OPAPP all documents and property of the same, including but not necessarily limited to: tables, project proposals, statistical data, and all other materials and all copies thereof relating in any way to OPAPP’s business, or in any way obtained by me during the course of employ. I further agree that I shall not retain copies, notes or abstracts of the foregoing;
 - b. OPAPP may notify any future or prospective employer or third party of the existence of this agreement, and shall be entitled to full injunctive relief for any breach; and,
 - c. This agreement shall be binding upon me and my personal representatives and successors in interest, and shall inure to the benefit of the OPAPP, its successors and assigns.

Signed this _____ day of _____, 2021.

NAME AND SIGNATURE OF EMPLOYEE
POSITION AND UNIT ASSIGNMENT

ANNEX D1
NON-DISCLOSURE AGREEMENT TEMPLATE FOR CONSULTANTS

Office of the President of the Philippines
OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS

NON-DISCLOSURE AGREEMENT

The **OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS**, herein referred to as “OPAPP” and the undersigned consultant or representative hereby agrees and acknowledges:

1. That during the course of my consultancy contract there may be disclosed to me certain information from OPAPP consisting of but not limited to:
 - a. Technical information: methods, processes, frameworks, compositions, research projects and publications.
 - b. Classified information: sensitive, confidential and privileged personal information, technical data in the possession of OPAPP that are considered as classified and/or confidential due to its implications on national security consisting of but not limited to data concerning the different Peace Processes of the Philippine Government.
2. I agree that I shall not during, or at any time after the termination of my contract with OPAPP, use for myself, or disclose or divulge to others including future employees, any trade secrets, confidential information, or any other proprietary data of OPAPP in violation of this agreement.
3. That upon the termination of my contract with OPAPP:
 - a. I shall return to OPAPP all documents and property of the same, including but not necessarily limited to: tables, project proposals, statistical data, and all other materials and all copies thereof relating in any way to OPAPP’s business, or in any way obtained by me during the course of contract. I further agree that I shall not retain copies, notes or abstracts of the foregoing;
 - b. OPAPP may notify any future or prospective employer or third party of the existence of this agreement, and shall be entitled to full injunctive relief for any breach; and,
 - c. This agreement shall be binding upon me and my personal representatives and successors in interest, and shall inure to the benefit of the OPAPP, its successors and assigns.

Signed this ____ day of _____, __ (year) __.

OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS	CONSULTANT/REPRESENTATIVE
NAME OF REPRESENTATIVE	NAME OF REPRESENTATIVE
Position	Position

ACKNOWLEDGMENT

Republic of the Philippines)

) S.S.

BEFORE ME, this _____ in _____, personally appeared the following:

NAME	GOVERNMENT ISSUED ID

who were identified by me through their competent evidence of identity to be the same persons who executed the foregoing document. Further, the parties acknowledged to me that the same is their true and voluntary act and deed, and the true and voluntary act and deed of the entities they represent, after the same document has been interpreted to them by me in a language and dialect known to them.

IN WITNESS WHEREOF, I have hereunto signed and affixed my notarial seal in the place and on the date first above written.

Doc. No. ____;

Page No. ____;

Book No. ____;

Series of ____;

ANNEX E¹ CONSENT FORM

We at the **OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS (OPAPP)** are committed to achieving just and lasting peace through the Philippine Comprehensive Peace Process, as mandated Executive Order No. 3, s. 2001 while implementing safeguards to protect your privacy and keep your personal data safe and secure.

Processing of Personal Data and Information

OPAPP shall collect, process, store, retain or destroy personal data including sensitive personal information for the purpose of _____ as governed by the provisions of the RA 10173 Data Privacy Act of 2012 and its Implementing Rules and Regulations.

Data Protection

OPAPP shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data which we collected.

The security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing

Confidentiality

OPAPP employees shall operate and hold personal data under strict confidentiality. They are required to sign non-disclosure agreements and are have received training on the agency's privacy and security policies to ensure confidentiality and security of personal data.

Rights of the Data Subjects

As Data Subject, you are entitled to the following rights:

- A. Be informed on whether your personal information shall be, are being or have been processed;***
- B. Be furnished with the information indicated below before the entry of your personal information into the processing system of the personal information controller, or at the next practical opportunity:***
 - 1. Description of the personal information to be entered into the system;
 - 2. Purposes for which they are being or are to be processed;
 - 3. Scope and method of the personal information processing;
 - 4. The recipients or classes of recipients to whom they are or may be disclosed;
 - 5. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;

¹ NPC Toolkit, "Elements of a Consent Guide"

**must be translated to the local language when necessary*

**applicable for participants 18 years old and older*

6. The identity and contact details of the personal information controller or its representative;
7. The period for which the information will be stored; and
8. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the National Privacy Commission.

Any information supplied or declaration made to you on these matters shall not be amended without prior notification: Provided, that the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, or when the information is being collected and processed as a result of legal obligation;

C. Reasonable access to, upon demand, the following:

1. Contents of your personal information that were processed;
2. Sources from which personal information were obtained;
3. Names and addresses of recipients of the personal information;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal information to recipients;
6. Information on automated processes where the data will or likely to be made as the sole basis for any decision significantly affecting or will affect you;
7. Date when your personal information was last accessed and modified; and
8. The designation, or name or identity and address of the personal information controller.

D. Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information has been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: Provided, that the third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon your request;

E. Suspend, withdraw or order the blocking, removal or destruction of your personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes or are no longer necessary for the purposes for which they were collected;

F. Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information; and,

G. Right to data portability, such that where personal information is processed by electronic means and in a structured and commonly used format, you have the right to obtain from the personal information controller a copy of data undergoing processing in an electronic or structured format, which is commonly used and allows for further use.

¹ NPC Toolkit, "Elements of a Consent Guide"

*must be translated to the local language when necessary

*applicable for participants 18 years old and older

Contact Information

If you have further questions or concerns, you may contact our Data Protection Officer through the following details:

Contact Number: _____

Email Address: _____

I have read this form, understood its contents and consent to the processing of my personal data. I understand that my consent does not preclude the existence of other criteria for lawful processing of personal data, and does not waive any of my rights under the Data Privacy Act of 2012 and other applicable laws.

Signature Over Printed Name
Date

OR

<p>RIGHT THUMB MARK HERE</p> <p>_____ Date</p>

Witness:

Signature Over Printed Name
Date

¹ NPC Toolkit, "Elements of a Consent Guide"

**must be translated to the local language when necessary*

**applicable for participants 18 years old and older*

ANNEX E1

ASSENT FORM

OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS

For OPAPP programs, projects and activities involving children (younger than 18 years old), an assent form must be administered by an OPAPP personnel directly involved in said endeavor. The contents of the form must be read aloud to the target participant in the presence of the parent/s or legal guardian. Agreement to participate may be signified through signing the form or stating a verbal affirmation. Verbal affirmations must be recorded, and stored with appropriate identification (name of child, date, time recorded)

Program/Project/Activity: _____

Implementing Department: _____

Inclusive Dates: _____

Name of OPAPP Representative/s: _____

1. What is the purpose of this Program/Project/Activity?

(State purpose)

2. Important things to know:

- *You get to decide if you want to take part.*
- *You can say 'No' or you can say 'Yes'.*
- *No one will be upset if you say 'No'.*
- *If you say 'Yes', you can always say 'No' later.*
- *You can say 'No' at any time.*
- *We would not take it against you no matter what you decide.*

3. What will I get if I participate?

(State benefits of the program/project/activity)

4. What can go wrong?

(State Risks)

If you agree to participate in this program/project/activity, you may write your name or tell me that you agree:

NAME: _____

(To be written by child/adolescent)

DATE: _____

TIME: _____

SIGNATURE OF OPAPP REPRESENTATIVE/s: _____

ANNEX E2¹

PARENTAL/LEGAL GUARDIAN CONSENT FORM

I/We, _____ and _____ of legal age,
single/married, Filipino citizen/s, and presently residing in
_____, parent/s/legal guardian/s of
_____ hereby consent to the participation of our child to the
(Program/Project/Activity) _____ organized/implemented by the
OFFICE OF THE PRESIDENTIAL ADVISER ON THE PEACE PROCESS.

SIGNATURE OVER PRINTED NAME/S OF PARENT/S/LEGAL GUARDIAN/S

DATE

SIGNATURE OVER PRINTED NAME OF OPAPP REPRESENTATIVE

¹ NPC Toolkit, "Elements of a Consent Guide"

*This form must be translated in the local language when necessary and shall be attached to the **Annex E1 ASSENT FORM.***

NATIONAL ARCHIVES OF THE PHILIPPINES

Pambansang Sinupan ng Pilipinas

GENERAL RECORDS DISPOSITION SCHEDULE

common to all Government Agencies

Series 2009

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
	<u>ADMINISTRATIVE and MANAGEMENT RECORDS</u>	
1	Acknowledgment Receipts	To be filed with appropriate records series
2	Brochures/Leaflets/Phamplets (About or by the agency)	1 year provided 1 copy is retained for reference
3	Calendars/Schedules of Activities or Events	1 year
4	Certificates of Appearance/Clearances	1 year
5	Certifications	1 year
6	Charts Functional Organizational	PERMANENT
7	Correspondences Non-routine Routine	To be filed with appropriate records series 2 years after acted upon
8	Delivery Receipts	2 years
9	Directories of Employees/Officials	2 years after superseded
10	Feasibility Studies	PERMANENT if implemented, otherwise dispose after 5 years from date of record
11	Gate Passes	6 months
12	Inquiries	2 years after acted upon
13	Issuances Issued by or for the head of agency documenting policies/functions/ programs of the agency Issued by or for the head of agency reflecting routine information or instruction	PERMANENT 2 years after superseded
14	Lists Associations Committees Cooperatives	1 year after updated

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
cont. 14	Lists Donors Mailing Transmittal Others	1 year after updated To be filed with appropriate records series
15	Logbooks Incoming/Outgoing Correspondences Visitors Ordinary VIP Others	2 years after date of last entry 2 years after date of last entry PERMANENT 2 years after date of last entry
16	Manuals	PERMANENT
17	Meetings/Proceedings Files Agenda Minutes Board/Executive Committee Staff Notices	1 year PERMANENT 1 year 1 year
18	Official Gazettes	PERMANENT
19	Permits	1 year after renewed/expired
20	Plans Action/Work Others	3 years after implemented PERMANENT if implemented, otherwise dispose 5 years from date of record
21	Press Releases (About or by the agency)	PERMANENT
22	Programs Work Others	3 years PERMANENT if implemented, otherwise dispose 5 years from date of record
23	Proposals	PERMANENT if implemented, otherwise dispose 5 years from date of record
24	Publications (Record Set)	PERMANENT
25	Reorganization Records	PERMANENT
26	Reports Annual/Special Others	PERMANENT 2 years after incorporated in the Annual Report

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
27	Requests	2 years after acted upon
28	Slips Locator Permission Routing	1 year
29	Speeches (Record Set)	PERMANENT
30	Standard Operating Procedures (SOP)	PERMANENT
31	Telegrams	1 year after acted upon
32	Trip Tickets	1 year
	<u>BUDGET RECORDS</u>	
33	Allotment Files Advices of Allotment (AA) Agency Budget Matrixes Allotment Release Orders General (GARO) Special (SARO) Obligation Request/Slips (ALOBS) Plan of Work and Requests for Allotment Registries of Allotment & Obligations (RAO) Capital Outlay (RAOCO) Financial Expenses (RAOFE) Maintenance & Other Operating Expenses (RAOMO) Personal Services (RAOPS) Requests for Obligation of Allotment (ROA) Statements of Allotment, Obligations & Balances (SAOB) Statements of Appropriations, Allotment & Advice (SAAA)	3 years 3 years 3 years 3 years 3 years 10 years 3 years 3 years 3 years
34	Annual Budgets	3 years
35	Budget Estimates Including Analysis Sheets and Estimates of Income	3 years
36	Budget Expenditures Programs Sources of Financing	5 years
37	Budget Issuances (Those used as authority for agency transactions)	10 years
38	Budget Sheet Analysis	3 years

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
39	Budgetary Ceilings	3 years
40	Cash Allocation Ceilings/Notices of Cash Allocation	3 years
41	Certifications of Funds Availability	1 year
42	General Appropriations Acts	3 years
43	Organizational Performance Indicator Framework (OPIF)	Permanent
44	Physical Reports of Operations	3 years
45	Special/Supplemental Budgets	3 years
46	Work and Financial Plans	3 years
	<u>FINANCIAL AND ACCOUNTING RECORDS</u>	
47	Abstracts	
	Daily Collections	5 years
	Deposits and Trust Funds	5 years
	General Collections	5 years
	Sub-Vouchers	2 years
48	Advices	
	Checks Issued & Cancelled	4 years
	Remittance	10 years
49	Annual Statements of Accounts Payable	PERMANENT
50	Auditor's Contract Cards	3 years
51	Authorities for Allowances	2 years after terminated
52	Authorizations	1 year after expired
	Overtime	
	Purchase of Equipment/Property	
	Transfer of Fund	
	Travel	
	Others	
53	Bank Slips	10 years
	Deposits	
	Remittances	
54	Bills	10 years after settled

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
55	Bonding Files Action Applications/Requests Fidelity/Surety Bond Indemnity for Issue of Due Warrant	3 years 3 years 5 years after expired/terminated 3 years
56	Books of Final Entry General Ledgers Subsidiary Ledgers	PERMANENT
57	Books of Original Entry Cash Disbursement Journals Cash Journals Cash Receipts Journals Check Disbursement Journals General Journals Journals of Analysis of Obligation Journals of Bill Rendered Journals of Check Issued Journals of Collection and Deposit Journals of Disbursement by Disbursing Officer	PERMANENT
58	Cash Flow Charts	PERMANENT
59	Certificates Settlement and Balances Shortages	10 years provided post-audited, finally settled and not involved in any case 10 years after settled
60	Claims Insurance Health Benefits Hospital	10 years after settled
61	Checks and Check Stubs	10 years provided post-audited, finally settled and not involved in any case
62	Daily Cash Flow	3 years
63	Daily Statement of Collections	5 years
64	Expense Ledgers	PERMANENT
65	Financial Statements Balance Sheets Income Statements Statements of Cash Flows (Annual) Statements of Operation	PERMANENT

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
66	Indices of Payments Creditors Employees Sundry Payments by Checks/Warrants	5 years 15 years after retired/separated PERMANENT
67	Journal Entry Vouchers	12 years provided post-audited, finally settled and not involved in any case
68	Lists of Remittances Loans Premiums	PERMANENT
69	Logbooks of General Funds	3 years after date of last entry
70	Monthly Settlements of Monthly Subsidiary Ledger Balance	2 years
71	Notices Disallowances Suspensions	3 years after settled
72	Official Cash Books	PERMANENT
73	Official Cash Books for Bank Cash Book	PERMANENT
74	Official Receipts	10 years provided post-audited, finally settled and not involved in any case
75	Orders of Payment	10 years
76	Payrolls	10 years provided post-audited, finally settled and not involved in any case
77	Payroll Payment Slips/Pay Slips	10 years
78	Quarterly Statements of Charges to Accounts Payable	10 years
79	Registry Books of Checks Released	PERMANENT
80	Registers Checks/Warrants Checks/Warrants Control	PERMANENT
81	Reliefs from Accountability Decisions Requests	10 years provided a copy is filed with 201 files
82	Reports Accountabilities for Accountable Forms Cash Disbursements Cash Examinations	3 years after cash had been examined 10 years 3 years provided post-audited, finally settled and not involved in any case

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
cont. 82	Reports <ul style="list-style-type: none"> Collecting & Disbursing Officers Checks Issued & Cancelled Collections & Deposits Disbursements Daily Cash Reports Liquidations Monthly Income Overdrafts and Misuse of Trust Funds Petty Cash Replenishments 	10 years provided post-audited, finally settled and not involved in any case 3 years 10 years 10 years 5 years after case had been settled or terminated 10 years provided post-audited, finally settled and not involved in any case
83	Schedules of Accounts Receivables	3 years
84	Statements <ul style="list-style-type: none"> Accounts <ul style="list-style-type: none"> Current Payable Receivable Common Funds Financial Conditions Profits and Losses Reconciliations 	3 years 10 years PERMANENT 10 years 10 years PERMANENT 10 years
85	Summaries of Unliquidated Obligations and Accounts Payable	10 years
86	Sundry Payments	10 years
87	Treasury Checking Accounts of Agency (TCAA)	10 years
88	Treasury Drafts	10 years
89	Treasury Warrants	10 years provided post-audited, finally settled and not involved in any case
90	Trial Balances and Supporting Schedules <ul style="list-style-type: none"> Cumulative Results of Operations-Unappropriated Final Annual Trial Balances <ul style="list-style-type: none"> Accounting's Copy Auditor's Copy Regional Office Copy Monthly/Quarterly Trial Balances Preliminary Trial Balances <ul style="list-style-type: none"> Accounting's Copy Auditor's Copy Regional Office's Copy 	PERMANENT 10 years after Annual Financial Report had been published PERMANENT 10 years after Annual Financial Report had been published 2 years after consolidated in the Annual Financial Report 10 years after Annual Financial Report had been published PERMANENT 10 years after Annual Financial Report had been published

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
91	Vouchers, including Bills, Invoices & Other Supporting Documents Disbursements Journals Petty Cash Reimbursement Expense Receipts Travelling Expenses	10 years provided post-audited, finally settled and not involved in any case for COA & Accounting Office/Department/ Division/Section/Unit. All other copies dispose after 1 year.
92	Withholding Tax Certificates	4 years after superseded
	<u>HUMAN RESOURCE/PERSONNEL MANAGEMENT RECORDS</u>	
93	Annual Summary Reports for Replacement Program for Non-Eligibles	5 years
94	Applications Employment Leave of Absence and Supporting Documents Relief of Accountability Retirement/Resignation	1 year 1 year after recorded in the leave cards 5 years after separated/retired 1 year
95	Attendance Monitoring Sheets	1 year
96	Authorities/Requests to Create or Fill Vacant Positions	2 years after vacant positions had been filled up
97	Certifications Employment Residency Service Others	1 year
98	Comparative Data Matrix of Employees	2 years
99	Daily Time Records	1 year after data had been posted in leave cards and post-audited
100	Employee Interview Records	1 year
101	Handwriting Specimens/Signature	PERMANENT
102	Job Order Employment Contracts	5 years after terminated
103	Leave Credit Cards	15 years after separated/retired
104	Lists of Eligibles/Non-Eligibles	1 year after updated
105	Logbooks Arrival & Departure of Employees Attendance Clearances Issued	2 years after date of last entry 1 year provided leave and undertimes are posted in the leave card 2 years after date of last entry

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
106	Medical Certificates in Support of Absence on Account of Illness/Maternity	3 years after absences had been recorded in leave cards
107	Membership Files GSIS Pag-ibig PhilHealth	15 years after separated/retired
108	Merit Promotion Plans	1 year after superseded
109	Performance Files Appraisal Evaluation Rating Cards Target Worksheets	1 year 1 year 5 years 1 year
110	Permissions to Engage in Business/Private Practice/Teach	2 years after expired
111	Personal Data Sheets (Curriculum Vitae/Resume)	1 year after superseded
112	Personnel Folders (201 Files) Appointments Acceptance of Resignation Approval of Retirement Awards Benefit/Gratuity Certificates Eligibility Rural Service Training/Seminar Attended Change of Marital Status/Name Clearance (latest) Designations/Details Oaths of Office Personal Data Sheet (latest) Position Descriptions Reinstatements Service Records (updated) Statements of Duties and Responsibilities	15 years after separated/retired
113	Plantilla of Personnel	PERMANENT while other copies dispose after 3 years
114	Position Allocation Lists	3 years
115	Position Classifications and Pay Plans	5 years after superseded
116	Recommendations/Referrals	1 year after acted upon

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
117	Reports Examinations Personnel Actions	2 years PERMANENT
118	Requests Accumulated Leave Credits Approval on Promotions Bonding Officials/Employees Changes of Status Reinstatements Transfers	1 year after acted upon/cleared
119	Salary Standardization Records	5 years after superseded
120	Staffing Patterns	PERMANENT
121	Service Cards	PERMANENT
122	Statements of Assets and Liabilities	10 years
	<u>LEGAL RECORDS</u>	
123	Administrative Cases	7 years after finally settled except Decisions which are Permanent
124	Affidavits	1 year after purpose had been served
125	Articles of Incorporation/By-Laws	PERMANENT
126	Complaints/Protests	5 years after settled
127	Contracts	5 years after renewed/terminated and/or finally settled
128	Decisions	PERMANENT
129	Deeds Donation Sale	PERMANENT
130	Legal Opinions	PERMANENT
131	Memoranda of Agreement/Understanding	PERMANENT
132	Petitions	5 years after settled
133	Resolutions	PERMANENT
134	Special Powers of Attorney	1 year after purpose had been served

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
135	Subpoenas Ad Testificandum Duces Tecum	3 years or to be filed with appropriate case
	<u>PROCUREMENT AND SUPPLY RECORDS</u>	
136	Acknowledgment Receipts for Equipment (ARE)/ Memorandum Receipts of Equipment (MRE), Semi-Expendable and Non-Expandable Properties	1 year after equipment had been returned
137	Annual Procurements Plans Programs	3 years
138	Bids and Awards Committee Files Abstracts Invitations Minutes Pre/Post Qualifications Publications Resolutions	5 years after contract of winner had been terminated/settled, others dispose after 1 year
139	Bills of Lading	2 years after delivery had been accepted
140	Bin Cards/Stock Cards on Supplies	3 years after date of last entry
141	Canvass of Prices	10 years if attached to vouchers, otherwise, dispose after 2 years
142	Equipment Ledger Cards	2 years after equipment had been disposed
143	Inventory and Inspection Reports of Unserviceable Properties	1 year after property had been disposed
144	Inventories of Equipment/Supplies	1 year after updated
145	Inventory Tag Cards	1 year after updated
146	Invoices / Receipts Accountable Forms Properties/Transfer of Properties	3 years after issuance of clearance had been terminated/after property had been returned
147	Invoices of Delivery on Supply Open-End Order Contracts	5 years
148	Job Orders	1 year
149	Lists of Supplies Under Supply Open-End	5 years
150	Monthly Reports of Supplies and Materials Issued	1 year

ITEM NUMBER	RECORDS SERIES TITLE AND DESCRIPTION	AUTHORIZED RETENTION PERIOD
151	Property Cards	PERMANENT
152	Purchase Orders	4 years
153	Purchase Requests	1 year
154	Queries on Prices of Articles, Additional Funds to Meet Quotations	1 year
155	Reports of Waste Materials	2 years
156	Requisition and Issue Slips/Requisition Issue Vouchers	1 year or file with appropriate records series
157	Shipping and Packing Lists on Items Purchased	1 year
158	Suppliers Identification Certificates with Procurement	2 years after renewed
159	Supplies Adjustment Sheets	1 year after post-audited
160	Supplies Availability Inquiries	1 year
161	Supplies Ledger Cards	5 years
162	Supplies Purchase Journals	5 years
	<u>TRAINING RECORDS</u>	
163	Calendars	1 year after superseded
164	Course Designs/Outlines/Syllabi	1 year after superseded
165	Masterlists Participants Seminars Conducted/Coordinated	PERMANENT
166	Resource Speaker Profiles	1 year after superseded
167	Schedules of Training/Seminar	1 year after superseded
168	Survey Evaluation Questionnaires	1 year after data had been evaluated
169	Training Handouts	1 year after superseded
170	Training Programs/Plans	3 years after superseded
171	Training Reports	2 years
172	Workshop Results	1 year

ANNEX G¹

Annual Security Incident Reports for PICs

SUMMARY

Annual Security Incident Reports

January to December 20__

Sector: _____ **City/Municipality:** _____ **Province:** _____

PIC (Individual or Organization): _____

Name of DPO: _____

PERSONAL INFORMATION CONTROLLER

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

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 : _____

¹NPC Advisory 18-02, "UPDATED TEMPLATES ON SECURITY INCIDENT AND PERSONAL DATA BREACH REPORTORIAL REQUIREMENTS"

ANNEX G1¹

Mandatory Notification: Personal Data Breach for the National Privacy Commission

<NAME OF ENTITY>

<ADDRESS>

<CONTACT INFORMATION>

<DATE>

<PRIVACY COMMISSIONER>

National Privacy
Commission Pasay City,
Metro Manila Philippines

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

Sir / Mesdames:

I write in behalf of <ENTITY>, in relation to the data breach of <DATE>, involving <BRIEF DESCRIPTION OF DATA>. This notification is made pursuant to the mandatory data breach notification procedure in Philippine law to the National Privacy Commission.

Responsible Officers. The pertinent details of <ENTITY>, and the responsible persons thereof, are as follows:

Head of the Organization	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
---------------------------------	---

Data Protection Officer	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
--------------------------------	---

Process Owner	<NAME> <OFFICE ADDRESS> <E-MAIL ADDRESS> <TELEPHONE> <OTHER CONTACT INFO>
----------------------	---

Nature of the Breach. In brief, we describe the nature of the incident, thus:

- Describe the nature of the personal data breach.
 - Be as specific as possible. Indicate if the details provided are sensitive to the entity, which may cause unwarranted damage to the entity if disclosed to the public.

¹NPC Advisory 18-02, "UPDATED TEMPLATES ON SECURITY INCIDENT AND PERSONAL DATA BREACH REPORTORIAL REQUIREMENTS"

- Provide a chronology that describes how the breach occurred; describe individually the events that led to the loss of control over the personal data.
- Provide a description of the vulnerability or vulnerabilities that of the data processing system that allowed the breach.
- Include description of safeguards in place that would minimize harm or mitigate the impact of the personal data breach.
- Indicate number of individuals or personal records affected. Provide an approximate if the actual impact has not been determined.
- Describe the likely consequences of the personal data breach. **Consider effect on company or agency, data subjects and public.**

Personal Data Possibly Involved.

- List all sensitive personal information involved, and the form in which they are stored or contained.
- Also list all other information involved that may be used to enable identity fraud.

Measures taken to Address the Breach.

- Describe in full the measures that were taken or proposed to be taken to address the breach.
- Describe how effective these measures are.
- Indicate whether the data placed at risk have been recovered. Otherwise, provide all measures being taken to secure or recover the personal data that were compromised.
- Indicate actions of the organization to minimize/mitigate the effect on the affected individual. Provide all actions being performed or proposed to mitigate or limit possible harm, negative consequences, damage or distress to those affected by the incident.
- Ensure the affected individuals are aware that the incident has occurred. Include all the actions being taken to inform the data subjects affected by the incident or any reasons for delay in the notification.
- Describe the steps the organization has taken to prevent a recurrence of the incident.

Should you require further information on this matter, contact us using the information above. Any information that later becomes available shall be reported within five (5) days, or as further required by the Commission.

Sincerely,
<ENTITY>

<HEAD OF AGENCY/
DATA PROTECTION OFFICER>

ANNEX G2¹

Mandatory Personal Data Breach Notification to Data Subjects

<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.

Please 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 shall provide more information to you as soon as they become available.

Sincerely,

<ENTITY>

<HEAD OF AGENCY/

<DATA PROTECTION OFFICER>





¹NPC Advisory 18-02, "UPDATED TEMPLATES ON SECURITY INCIDENT AND PERSONAL DATA BREACH REPORTORIAL REQUIREMENTS"

OFFICE OF THE PRESIDENT OF THE PHILIPPINES
Office of the Presidential Adviser on the Peace Process



Privacy Management Framework



 INPUTS	 PROCESSES	 OUTPUTS	 OUTCOME/GOAL
<ul style="list-style-type: none"> ✓Data Privacy Act and other Privacy guidelines and issuances ✓Management and Organizational Commitment 	PILLAR 1: Designation of Privacy Compliance Officers 1. Identification of personnel to be designated as Data Protection Officer (DPO) and alternate, and as members of the Privacy Compliance Teams (Composite Team (CT), and Department Privacy/Area Management Office Privacy Focal persons (DPFs)) 2. Official designation of identified/nominated personnel through an office order	<ul style="list-style-type: none"> ✓Privacy Compliance Officer (Data Protection Officer (DPO, Alternate) and Privacy Compliance Teams (Composite Team (CT), and Department Privacy/Area Management Office Privacy Focal persons (DPFs) designated 	Respect for Privacy embedded in all of OPAPP's PPAs, and Processes, and Privacy Resiliency achieved
<ul style="list-style-type: none"> ✓Data Privacy Act and other Privacy guidelines and issuances ✓Management and Organizational Commitment ✓Programs, Projects, and Activities (PPAs), and Systems processing Personal Data and Information ✓Funding 	PILLAR 2: Privacy Impact Assessment (PIAs) 1. Inventory of personal data and information processing activities 2. Privacy Risk Assessment 3. Identification of Privacy Gaps 4. Formulation of appropriate recommendations to address identified gap.	<ul style="list-style-type: none"> ✓Department and Organizational PIAs regularly conducted. 	
<ul style="list-style-type: none"> ✓Data Privacy Act and other Privacy guidelines and issuances ✓Management and Organizational Commitment ✓Initial Results of the PIA 	PILLAR 3: Privacy Manual and Privacy Management Framework 1. Review of the Initial Results of the PIA and all available privacy-related policies. 2. Identification of applicable data and information security measures and controls. 3. Development of Privacy Manual and Privacy Management Framework.	<ul style="list-style-type: none"> ✓Privacy Manual and Privacy Management Framework developed and Approved. 	
<ul style="list-style-type: none"> ✓Data Privacy Act and other Privacy guidelines and issuances ✓Management and Organizational Commitment ✓Approved Privacy Manual containing Data and Information Security Measures ✓Approved Privacy Management Framework ✓Funding 	PILLAR 4: Data and Information Security Measures and Protocols 1. Operationalization of Privacy Manual and Privacy Management Framework through implementation of organizational, physical, and technical security measures. 2. Development and conduct of privacy-related internal policies, directives and activities. 3. Agency Registration of Privacy Compliance Officers and Personal Data and Information Processing Activities 4. Agency Compliance and Implementation Monitoring 5. Privacy Policy Review, Updating and Enhancements	<ul style="list-style-type: none"> ✓Data and Information Security Measures and Protocols implemented, Assessed, and Updated. 	
<ul style="list-style-type: none"> ✓Data Privacy Act and other Privacy guidelines and issuances ✓Management and Organizational Commitment ✓Approved Privacy Manual containing Data and Information Security Measures ✓Approved Privacy Management Framework ✓Developed Privacy-related Internal Policies and directives ✓Funding 	PILLAR 5: Breach Response Management 1. Designation of Breach Response Team (BRT) 2. Capacity-building of Privacy Compliance Officers and Teams on Breach and Security Incident Response. 3. Conduct of PIA, and regular breach response drills. 4. Documentation of Breach and Security Incidents	<ul style="list-style-type: none"> ✓Breach Response Management regularly exercised. 	



Office of the President of the Philippines
Office of the Presidential Adviser on the Peace Process
7/F, Agustin 1 Bldg F, Ortigas Jr. Road, Ortigas Center, Pasig City • Tel. No.: 6360701 • Fax No. 6382216

Office Order
No. 081
Series of 2021

**SUBJECT: OPERATIONALIZATION OF THE DATA PRIVACY MANUAL AND
PRIVACY MANAGEMENT FRAMEWORK**

In compliance to the Republic Act 10173 also known as the Data Privacy Act of 2012, which instructs all government agencies, as personal information controller, to set forth security measures for the protection personal data and information, this is to operationalize the approved Data Privacy Manual and Privacy Management Framework and mandate all members of OPAPP to adopt and implement the measures contained therein.


Anchored in the principles of data privacy, namely, transparency, legitimate purpose, proportionality, the Data Privacy Manual and Privacy Management Framework shall lead OPAPP towards a culture protective of data privacy rights of all internal and external stakeholders, through laying down physical, technical and organization data and information security measures and mechanisms.

The Data Privacy Manual and Privacy Management Framework is OPAPP's commitment to uphold the rights to privacy of its clients and stakeholders, in furtherance of the agency's mandate to oversee, coordinate and integrate the implementation of the comprehensive peace process, and in the relentless pursuit of a just and enduring peace for all Filipinos.

This Office Order shall take effect immediately and shall remain in force unless otherwise revoked or modified.

Issued this 29th day of September 2021, in Ortigas Center, Pasig City.

SECRETARY CARLITO G. GALVEZ, JR.
Presidential Adviser on Peace, Reconciliation and Unity

 9/29/21
(CERTIFIED TRUE COPY
FROM THE ORIGINAL RECORD ON FILE)