



ENHANCED OPAPRU **DATA PRIVACY MANUAL AND PRIVACY MANAGEMENT FRAMEWORK**

Series of 2023



TABLE OF CONTENTS

I.	Introduction.....	3
II.	Definition of Terms.....	3
III.	Governing Policies and Programs.....	4
IV.	Scope and Limitation.....	5
V.	Privacy Management Framework.....	5
VI.	Personal Data and Information Processing Protocols.....	7
VII.	Security Measures.....	14
VIII.	Breach and Security Incidents.....	22
IX.	Inquiries and Complaints.....	24
X.	Annexes.....	26



Office of the President of the Philippines
Office of the Presidential Adviser on Peace, Reconciliation and Unity
7th Floor, Agustin I Building, F. Ortigas Jr. Ortigas Center, 1605 Pasig City Tel (+632) 636-0701 Fax No: (+632) 638-2216



ENHANCED OPAPRU DATA PRIVACY MANUAL AND PRIVACY MANAGEMENT FRAMEWORK

Series of 2023



Approved/~~Disapproved~~:

A blue ink signature of Carlito G. Galvez, Jr. written over the "Approved/Disapproved" text.

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

I. INTRODUCTION

The Office of the Presidential Adviser on Peace, Reconciliation, and Unity (OPAPRU) has remained steadfast in its aim to continuously foster a culture of respect for data and information privacy. Since the institutionalization of the OPAPRU's data and information privacy policies in 2021, the Agency has made landmark internal policies, projects, and activities, all geared towards building OPAPRU's capacity to ensure the protection of its stakeholders, and as part of the flagship initiatives to uphold the **General Data Privacy Principles of transparency, legitimate purpose, and proportionality**.

In furtherance of the aim to provide its stakeholders with uninterrupted, adaptive, and robust data and information protection services, the OPAPRU shall endeavor to sustain the maintenance and implementation of this Privacy Manual. The provisions of this document are anchored on 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). This Manual shall institutionalize updated guidance on the Agency's protocol and measures on data protection and shall serve as a handbook for the OPAPRU personnel in ensuring the Agency's compliance with the DPA, all towards the goal of nurturing a culture that values and promotes the right to privacy.

II. DEFINITION OF TERMS¹

A. Data Protection Officer (DPO)

The official of OPAPRU 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.

F. 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.

G. Privacy Impact Assessment

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

H. 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 OPAPRU shall be governed by the following policies:

1. R.A. 10173 "*Data Privacy Act of 2012*"
2. R.A. 9470 "*The National Archives of the Philippines Act of 2007*"
3. 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 Therefor*"
4. Memorandum from the Executive Secretary dated 24 November 2016, "*Inventory of Exceptions to E.O. 2 s. 2016*"
5. E.O. 608, s. 2007 "*Establishing a National Security Clearance System for Government Personnel with Access to Classified Matters and for Other Purposes*"
6. ISO/IEC 27001 International Standard on Information Security Management

7. ISO/IEC 27701 International Standard on Personal Identifiable Information (PII)
8. ISO 27032 International Standard on Cybersecurity Management
9. ISO 31000 International Standard on Risk Management
10. ISO 22301 International Standard on Business Continuity Management System (BCMS)
11. Policies, Guidelines, and Frameworks of OPAPRU
12. Laws and Regulations that may repeal the foregoing

IV. SCOPE AND LIMITATION

This Manual shall govern all acts pertaining to personal data and information of OPAPRU’s partners, stakeholders, outsources, donors, beneficiaries, resource persons, consultants, contractual employees and officers, personnel engaged through Contract of Service (CoS), retired personnel, applicants, contract counterparties and other persons whose personal data are directly or indirectly processed by OPAPRU and offices, services, units, and area management units (AMUs), collectively known as “*OPAPRU Data Subjects*”.

V. PRIVACY MANAGEMENT FRAMEWORK

The OPAPRU’s pursuit of the continued implementation and maintenance of its privacy policies, measures, and protocols shall be guided by the Privacy Management Framework (PMF). The PMF outlines the requirements to operationalize and comply with the DPA, its IRR, and all issuances set forth by the National Privacy Commission, all towards the desired outputs, outcomes, and the goal of nurturing an environment where the culture of respect for privacy may flourish.

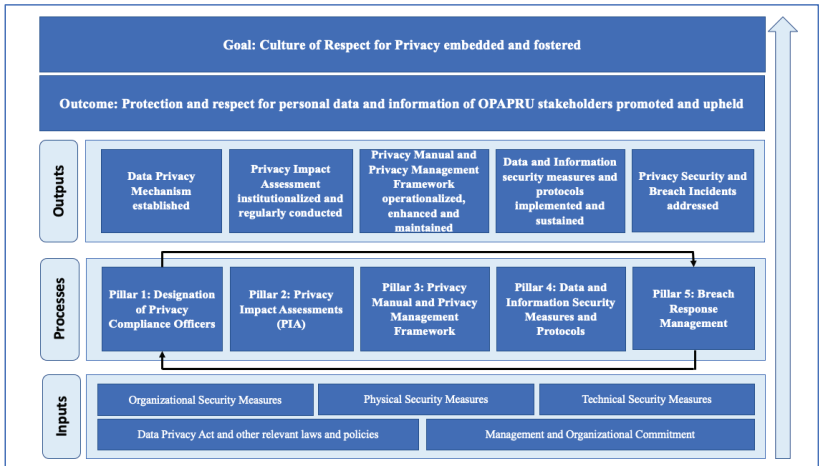


Figure 1. Privacy Management Framework

The achievement of the OPAPRU’s goal in terms of its privacy compliance takes root in the creation of enabling spaces and mechanisms to allow all policy-mandated technical, physical, and organizational security measures to be effectively implemented. The execution of all Agency privacy interventions and protocols shall be in line with the **Five Pillars of Data Privacy Compliance** and its corresponding activities and requirements which are as follows:

Table 1: Five Pillars of Data Privacy Compliance

Pillar	Requirements/Activities
Pillar 1: Designation of Privacy Compliance Officers (PCO)	<ul style="list-style-type: none"> • Identification and official designation of personnel/officers to serve as members of the PCO
Pillar 2: Privacy Impact Assessment (PIA)	<ul style="list-style-type: none"> • Institutionalization of PIA as a requirement for approval of systems, programs, projects, and activities, that would directly or indirectly process personal data and information
Pillar 3: Privacy Manual and Privacy Management Framework	<ul style="list-style-type: none"> • Implementation and maintenance of approved privacy manual and privacy management framework
Pillar 4: Data and Information Security Measures and Protocols	<ul style="list-style-type: none"> • Maintenance of established privacy security measures and protocols • Formulation of internal privacy policies anchored on the Agency Data Privacy Manual and other relevant issuances of the NPC • Agency registration with the NPC of the designated PCO, and ongoing systems processing personal data and information • Review of existing privacy measures, protocols and policies
Pillar 5: Breach Response Management	<ul style="list-style-type: none"> • Establishment of the Breach Response Team (BRT) • Continued capacity building of the Privacy Compliance Officers • Conduct of PIA to all applicable Agency activities, and breach response drills • Documentation and reporting of breach and information security incidents

The achievement of all the pillars shall lead to complementary and interdependent outputs, namely; data privacy mechanism established, PIA institutionalized and regularly conducted, data and information security measures and protocols implemented and sustained, and data security and breach incidents addressed. To ensure the sustainability of the framework and privacy-related OPAPRU issuances

and policies, the Five Pillars of Data Privacy Compliance shall be implemented in a cyclic nature, meaning, the pillars as well as their requirements and activities, shall be maintained and evaluated for Agency compliance on an annual basis.

VI. PERSONAL DATA AND INFORMATION PROCESSING PROTOCOLS

The OPAPRU, its offices, services, units, and AMUs, process personal data and information in accordance to its mandate to manage, direct, integrate, and supervise the implementation of the Comprehensive Peace Process through promoting and reinforcing reconciliation and unity among the Filipino people. To this end, the OPAPRU shall adhere to the following protocols to ensure a whole-of-agency approach in complying with the DPA:

A. Principles of Processing Personal Data and Information²

The OPAPRU shall be committed to adhering to four general principles with respect to the collection and processing of personal data:

1. **Transparency** – ensure that the OPAPRU Data Subjects are aware of the nature, purpose, and extent of the processing of their 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** – 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. **Data Quality** – ensure that data are accurate and where necessary for declared, specified, and legitimate purposes, kept up to date. Inaccurate data must be rectified, supplemented, destroyed or their further processing restricted.
4. **Proportionality** – 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

The Agency 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 158, s. 2021.

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

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

2. Protection of privacy rights and welfare of OPAPRU 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, OPAPRU 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 operations of OPAPRU offices, services, units, and AMUs, including administrative and technical operations, among others;
3. Management of human resources, including external sources of technical service providers and prospective human resources;
4. OPAPRU data subjects external and internal affairs and relations;
5. Database and records keeping and maintenance;
6. Research and documentations;
7. Media coverage;
8. Agency 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 Privacy Notice contains a list of 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 of OPAPRU (*See Annex A for the Privacy Notice*). The Notice shall be uploaded in the website, official social media accounts, as well as all systems designed to generate and process personal data and information of OPAPRU. 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 Peace, Reconciliation and Unity (OPAPRU), mandated to manage, direct, integrate, and supervise the implementation of the Comprehensive Peace Process through promoting and reinforcing reconciliation and unity among the Filipino people, is committed to continue upholding the right to privacy of all OPAPRU 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 this platform. OPAPRU shall ensure the confidentiality of personal data and information collected through appropriate security measures.

D. Personal Data and Information Collected and Methods of Collection

The OPAPRU 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, the 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. attorney’s opinion/advice to an individual, priest-individual conversations, physician-patient conversations, new information developed from investigations)*.

The collection methods for these types of information include digital/physical formats of official communications, document submissions, personal data sheets, registration forms, reports, databases, and research and data gathering tools (survey forms, key informant interviews, focus group discussions), and

consultations and dialogues, among others, and are collected/received by authorized OPAPRU personnel, officers, and legitimate partners.

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

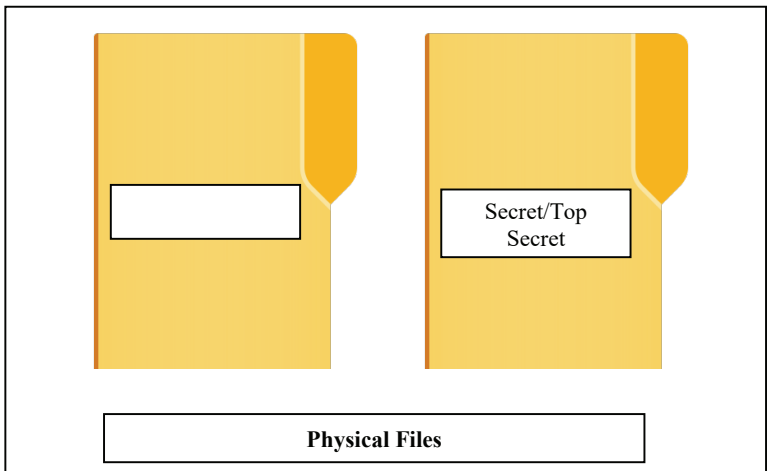
The OPAPRU processes personal data and information in line with the stipulations of the DPA 2012 and its IRR, and in accordance with the current operational dynamics of the Agency as it continues to execute its mandates. These personal data and information are contained in varying digital and physical formats and possess different levels of privacy sensitivities which require a diverse authority of access.

Table 2: Data and Information Classification and Authority of Access Matrix

Data and Information Classification/Prescribed Label	Authority of Access	Sample Files/Records/Documents
<p>For General Circulation and Access</p> <p>All records, files, and documents containing personal data and information, in Physical or Digital format, mandated by law to be publicized, or authorized by the OPAPRU officials for release and publication to various dissemination platforms available</p>	<p>General Public</p>	<p>Program, Project, and Activities (PPA) Progress/Accomplishment and Terminal Reports, Statement of Assets, Liabilities and Net Worth (SALN) <i>(upon request)</i>, OPAPRU Agency Directory, Media Coverage Reports</p>
<p>Confidential</p> <p>All records, files, and documents, containing personal data and information, 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>Restricted to OPAPRU personnel only</p>	<p>Database of peace partners, and actors, OPAPRU organized activity resource persons, and participants, official communications labelled as confidential building visitors, employee 201 files, database and profiles of OPAPRU's Program, Project, Activities (PPA) beneficiaries and stakeholders, meeting recordings.</p>
<p>Top Secret</p>	<p>Restricted to the executive and</p>	<p>Official communications labeled as Secret/ Top</p>

Data and Information Classification/Prescribed Label	Authority of Access	Sample Files/Records/Documents
All records, files, and documents, containing personal data and information, 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 OPAPRU labeled as "Secret" or "Top Secret"	management officials, and specific OPAPRU personnel addressee	Secret, database of OPAPRU partners, reports and database of members of active armed groups, legal case files, amnesty records, court rulings and proceedings, national security and surveillance reports

All physical records, files, and documents containing personal data and information must be enclosed in folders with the indicated **Prescribed Labels** for internal and external transmittals. Email subjects containing personal data and information shall likewise indicate agency data classification to control personnel and non-personnel access. Labeling standards are shown below:



From	peacemonth@peace.gov.ph	Bcc
To	insg.nscs@gmail.com X	
Cc		
CONFIDENTIAL/SECRET: xxxxxxxxxxxxSUBJECT:xxxxxxxxxxxxxxxx		
Email Subject Label		

Figures 2.a and b. Standard Labelling

F. Internal and External Data and Information Sharing

The OPAPRU shall safeguard internal and external disclosure of files, records, and documents containing personal data and information through the implementation of privacy controls to limit and control access and prevent unauthorized disclosure and access. All **Internal Data and Information Sharing** shall be protected by the internal privacy policies, and shall be overseen by the PCOs, technical and administrative staff, as authorized by the respective heads.

For **External Data and Information Sharing**, there must be an **official letter of request** from the requesting party supplemented by a **Data Request Form (See Annex B)**, along with the list of personnel who will gain access of the requested data and information. All Data Request Forms shall be processed by the concerned offices, services and units, and evaluated accordingly and approved by the its head. It must however be noted that the **processing, including distribution, of sensitive personal information and privileged information shall be prohibited, except for the cases as provided for in Section 13⁴ of RA 10173 or the Data Privacy Act of 2012 and the provisions**

⁴ **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

set forth by the Memorandum from the Executive Secretary dated 24 November 2016 or the Inventory of Exceptions to Executive Order No. 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.”

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 with 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 OPAPRU or deleted from the other party’s database. Further, **all Memoranda of Agreements (MOAs) 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 the Agency, are kept confidential and protected.

Moreover, **all, except those classified as for General Circulation** records, files, and documents 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. The OPAPRU 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 OPAPRU. The concerned office, service, or unit shall process and conduct validation of the said request.

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

Table 3: Internal and External Sharing Requirements

Type of Request	Requirements
Internal (Within OPAPRU, Inter-Unit)	None
External (Outside OPAPRU)	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
Owner of the personal data and information (e.g., amnesty certificate)	Letter addressed to OPAPRU

G. Outsourcing and Subcontracting of OPAPRU Data Subjects Personal Data and Information

The Agency 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 OPAPRU Data subjects shall also be governed by the rules and regulations under the *DPA IRR Rule X, Section 44 "Agreements for Outsourcing."*

VII. SECURITY MEASURES⁵

To complement the abovementioned protocols, the OPAPRU shall likewise implement various measures to protect its organizational assets and operations, and continuously uphold its stakeholders’ right to privacy. The following measures shall be strictly adhered to by all OPAPRU personnel in processing personal data and information:

A. Organizational Measures

The Agency shall execute the following measures to protect the **human aspect of data privacy**:

1. Privacy Impact Assessment (PIA)

The OPAPRU shall integrate the PIA into the project management cycle of Programs, Projects, and Activities (PPAs) and systems which shall process the personal data and information of OPAPRU data subjects. This shall be pursued through an **office order requiring an attached PIA in all relevant PPAs and systems included in the memorandum for approval**. The PIA shall ensure that all initiatives of the Agency are evaluated for their privacy risks and that all necessary steps to mitigate anticipated risks are in place before the PPAs or systems are implemented.

2. Designation, Updating and Mobilization of Data Privacy Mechanism

To ensure the compliance of the Agency with the DPA 2012, its IRR and all relevant NPC issuances, the OPAPRU shall designate and operationalize the following through an office order:

⁵ R.A. 10173, IRR, Rule No. 6, “Security Measures for Protection of Personal Data”

a. Data Protection Officer (DPO) and Alternate

The DPO of OPAPRU and his or her alternate shall have the ranks of Assistant Secretary and Director, respectively, and shall take on the following responsibilities as prescribed by the NPC:

- i. Monitor the OPAPRUs and the contracted PIP compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies. For this purpose, he or she may:
 - Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the OPAPRU or PIP, and maintain a record thereof;
 - Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
 - Inform, advise, and issue recommendations to the OPAPRU or PIP relative to data protection;
 - Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and,
 - Advise the OPAPRU or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensuring its compliance with the law.
- ii. Ensure the conduct of PIAs relative to activities, measures, projects, programs, or systems of the OPAPRU or PIP;
- iii. Advise the OPAPRU 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);
- iv. Ensure proper data breach and security incident management by the OPAPRU 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;
- v. Inform and cultivate awareness of privacy and data protection within the organization of the OPAPRU or PIP, including all relevant laws, rules and regulations, and issuances of the NPC;
- vi. Advocate for the development, review, and/or revision of policies, guidelines, projects, and/or programs of the OPAPRU or PIP relating to privacy and data protection, by adopting a privacy-by-design approach;
- vii. Serve as the contact person of the OPAPRU 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 OPAPRU or PIP;

- viii. Cooperate, coordinate, and seek the advice of the NPC regarding matters concerning data privacy and security; and
- ix. Perform other duties and tasks that may be assigned by the head of the OPAPRU that will ensure data privacy and security and uphold the rights of the data subjects.

b. Composite Team (CT)

The agency shall establish a CT to assist the DPO and his or her alternate in performing their duties. The team shall be comprised of members from various units, and shall execute the following functions and responsibilities.

- i. Assist in the monitoring and compliance of the agency's compliance to the DPA;
- ii. Coordinate with the Breach Response Team in case there are complaints received on data breaches; and;
- iii. Perform other duties and tasks as may be assigned by the DPO in relation to data protection and security.

c. Privacy Compliance Officers (PCO)

To further ensure compliance with the DPA 2012 down to the smallest unit of the Agency, and nurture the culture of respect for privacy up to the individual level, the OPAPRU offices, services, and units shall be represented by their respective PCOs. The PCO may be a junior or senior technical staff, tasked to represent their respective units in privacy-related activities. The designated personnel shall undertake the following functions:

- i. Join the DPO, his/her alternate, CT, and the 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.
- ii. Participate in all activities relating to Data Privacy including meetings, drills, learning sessions;
- iii. Participate and provide inputs and recommendations on the establishment of the OPAPRU's Records Section in compliance with the DPA 2012 and R.A. 9470 the National Archives of the Philippines Act of 2007.
- iv. Ensure adherence to privacy measures and protocols, monitoring and reporting security incidents, such as data breaches and privacy concerns, within their department/division/office.



d. Breach Response Team (BRT)

To ensure a dedicated sub-mechanism to address data and information security incidents, a Breach Response Team (BRT) shall be established. The BRT shall effectively execute the following functions:

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

The fulfillment of the respective roles and responsibilities shall be accounted for in the respective personnel's Individual Performance Commitment Report (IPCR).

3. Non-Disclosure Agreement (NDA) Requirement for all Personnel, Technical and Administrative Consultants, and Service Providers

All personnel, contractual and engaged in contracts of service (CoS), and job orders (JO), from the central office and AMUs, shall be required to sign a **Non-Disclosure Agreement (NDA) for Employees (Annex D)**. All personnel processing personal data and information shall strictly keep OPAPRU's data and information confidential, even after retirement and resignation. All service providers and technical consultants who shall collect and process personal data and information shall likewise sign an **NDA for Consultants (Annex D1)**. The NDAs shall be attached to all contracts issued by OPAPRU.

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

To continuously build and develop capacity and enhance knowledge of OPAPRU 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 breaches, the following are the training themes to which all the training designs are to be anchored in:

Table 4: Privacy-related Training Themes

Themes	Target Beneficiaries
OPAPRU Data Privacy Manual and Privacy Management Framework	All OPAPRU Personnel and Data Privacy Mechanism
Training on the use of the NPC Toolkit for the Conduct of Department Privacy Impact Assessments	
Data Information and Cybersecurity Learning Sessions	
Physical Data and Information Handling and Archiving	OPAPRU 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	OPAPRU Administrative Officers and Assistants, Central Routing Personnel
Breach Response Training	Breach Response Team

5. Activity Documentation and Recording

The Agency shall maintain accurate and appropriate documentation and recordings of all activities, systems, and processes, utilizing prescribed OPAPRU documentation templates and in accordance with the principles of data privacy. The documentation and recordings must be kept on file in a safe and secure repository and shall be kept confidential at all times. Verbal and written consent for media coverage, interviews, research purposes, and photo documentation, must at all times be secured through the prescribed **assent (for 18 years old and below) and consent forms**, translated into local languages, when necessary (**Annex E, E1, E2**). For interventions requiring the processing of personal data of children, child safeguards according to Philippine and international standards must be put in place by the office, service or unit of primary responsibility.

6. Compliance Internal Audit and Assurance

To ensure that OPAPRU's measures and policies are compliant with the DPA, the Agency shall mobilize the PCOs to conduct regular security checkpoints within their respective units, and report to the DPO and CT all activities that are not aligned with the agency policies on data privacy. Further, through the Data Privacy Mechanism, OPAPRU shall register to the NPC all systems and processes currently being operationalized in the organization and the composition of the privacy mechanism for recording and monitoring purposes. When necessary, the Agency shall engage an external data privacy auditor, to assess OPAPRU's compliance with the DPA. The agency shall also prepare for NPC-initiated compliance, privacy sweeps, and onsite visits.

B. Physical Measures

The Agency's protection of data and information from various threats include securing its physical assets including equipment, storage containers and facilities, work stations, and building perimeters. Towards this end the personnel shall adhere to the following physical measures:

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

The personal data and information collected by the OPAPRU may either be in digital/electronic or physical/paper-based format. Files, records, and documents in these formats may require varying storage facilities to protect contained data. The following measures must be followed when storing, retaining, and disposing of personal data and information:

Table 5: Storage, Retention and Disposal Measures

Format	Storage Type and Location	Retention	Disposal
Physical/Paper-based	Filing cabinets, water-proof, file folders, binders, file cases, laterals, etc. within OPAPRU building/premises.	As necessary, as prescribed by R.A. 9470 or the National Archives of the Philippines (NAP) Act of 2007 (See Annex F for the NAP Circular 2: Prescribed retention periods for each specific record), as authorized by OPAPRU officials	Upon authorization of relevant OPAPRU officials, or upon reaching the prescribed retention period of NAP, through shredding and incineration.
Electronic/Digital	OPAPRU servers, Agency-managed online storage, Agency-issued storage device		Upon authorization of relevant OPAPRU officials, or upon reaching the prescribed retention period of NAP, through device reformatting, complete manual and remote deletion.

Further, scanned copies of all physical/paper-based files must be secured for backup, these duplicates shall then be stored in authorized storage facilities and devices for digital copies. In all of the storage types and locations, appropriate labels must be indicated for ease of retrieval and tracking.

2. Access Procedure of Agency Personnel

The Agency shall further restrict access to physical files and storage devices to authorized personnel. To track and monitor personnel access, offices, services, and units shall maintain physical logbooks containing the following details:

- a. File Name
- b. Date and Time of Access
- c. Name of Personnel
- d. Purpose of Access
- e. Date and Time of return

Log books must be monitored regularly by the designated authorized personnel. Physical files taken out of the room/file cabinet must be authorized, cleared by the designated personnel, and returned immediately. It is also prohibited for unauthorized personnel to keep physical or digital copies of documents containing personal data and information, without prior authorization.

3. Clean Work Station Policy

All OPAPRU personnel shall adhere to the 5S workplace organization scheme—sort, set in order, shine, standardize, and sustain, during and after a work shift, in accordance with ISO 9001:2015. The 5S directs all to:

- a. Sort – separate needed from unneeded items, eliminate what isn't needed
- b. Set in Order – neatly arrange what is left after sorting – a place for everything, everything in its place
- c. Shine – clean, wipe & inspect the work area
- d. Standardize – create a standard practice for the above, this results in cleanliness from the regular performance of the first three “S”
- e. Sustain – continuously perform the first four “S”

Additionally, work equipment, including computer monitors, must be cleared during break times and at the end of the work day to avoid a data privacy breach. Digital and physical files must not be exposed in plain view, and all devices used for personal data and information processing must be password protected.

4. Field Work Station Protocols

All personnel on official fieldwork 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 a secured and discreet container to avoid unauthorized viewing.

5. Equipment Inventory and Check-Ups

All offices, services, and units, through their designated PCO and administrative officer, in collaboration with the Administrative Service, shall conduct an 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).

6. Privacy-promoting Work Areas

Workstations in OPAPRU must be designed to ensure privacy. Computer screens must not face the entrance of the office to avoid unauthorized persons/guests from viewing files/details of working files. Ample spaces between each workstation must also be maintained.

7. Building and Perimeter Security

The Agency's building, both in the central office and AMUs must be restricted to its personnel and authorized guests to further prevent data and information security breaches. The whole office perimeter must have security cameras recording 24/7, with its footage 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

The OPAPRU shall lay down technical measures to protect agency networks where the majority of personal data and information processing activities take place. The following measures are to be implemented and adopted, either spearheaded by or in collaboration with the ICT Division:

1. Software installation protocol

The Agency shall ensure that software installation to all agency-owned equipment and devices is monitored to ensure the prevention of encroachment of unauthorized software in agency-issued devices. All available reliable anti-virus applications shall be installed in all devices used in personal data and information processing.

2. Vulnerability Assessment

Within the resources of the Agency, OPAPRU shall test and evaluate all systems used in processing personal data and information for their reliability and security through a vulnerability assessment (VA). The VA shall either utilize free, open-source, but reliable software or may use paid licenses to execute the assessments. The results of the VA shall be used as a basis to

come up with remedying measures for the identified privacy gaps and concerns.

3. 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 the official OPAPRU email address as stipulated in the Office Order on Email Communication issued in 2022. Files must be password-protected using the data encryption tools available. Passwords of encrypted files may be shared with 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, coupled with the appropriate subject labels as indicated in *Chapter VI, Section E. Agency Data and Information Classification, Disclosure, and Authority of Access*.

VIII. BREACH AND SECURITY INCIDENTS⁶

Despite all the measures and protocols in place, there is still a possibility that data and information breach and security incidents will happen. To ensure that the agency is capacitated to respond to these incidents, and equipped with the necessary technologies and innovations to properly address, mitigate, remedy, and prevent information security concerns, the following are to be implemented:

A. Operationalization and Capacitation of the Breach Response Team (BRT)

Towards this end, the OPAPRU shall ramp up its efforts to ensure that the Data Privacy Mechanism is mobilized, especially the BRT, in appropriately responding to privacy threats. Regular coordination meetings, including the PCOs, DPO, and CT, shall be conducted to effectively address matters relating to breaches. Trainings and drills for breach response shall regularly be hosted and facilitated by internal or outsourced experts.

B. Data and Information Breach Preventive Actions

The Agency, through the BRT shall regularly conduct perimeter check-ups, network scanning, and provision of trainings to the personnel directly involved in the processing of personal data and information. **Regular breach response drills/learning sessions and trainings** participated in by the PCOs and the BRT, shall be conducted to better prepare the agency in responding to breach and security incidents.

C. Monitoring of Security Breaches

Regular operational monitoring of possible and anticipated security breaches shall be implemented by the data privacy mechanism, particularly the BRT. The Agency shall likewise further utilize available firewall software to alert the

⁶ R.A. 10173, IRR, Rule No. 9, “Data Breach Notification”, NPC Circular 16-03 – Personal Data Breach Management

organization of any attempt to interrupt or disturb the system and networks. All potential and identified data and information breaches shall be documented and addressed accordingly.

D. Back-Up and Restoration of Personal Data and Information

To be ensured by the PCOs and designated administrative and technical officers, 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. 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.

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

Addressing privacy security breaches begins with an incident report from all involved offices, services, and units, 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 OPAPRU data subjects. OPAPRU's personal data breach reporting structure shall be as follows:

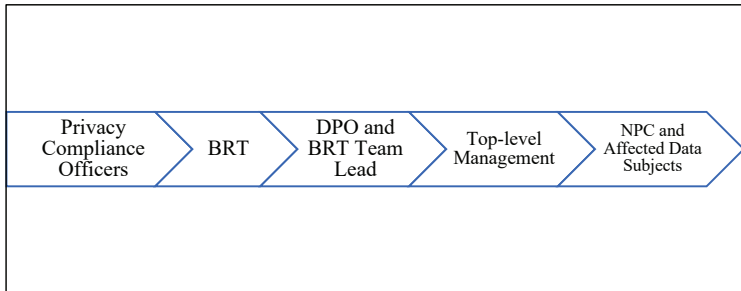


Figure 3. Privacy Security Incidents and Breaches Reporting Structure

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

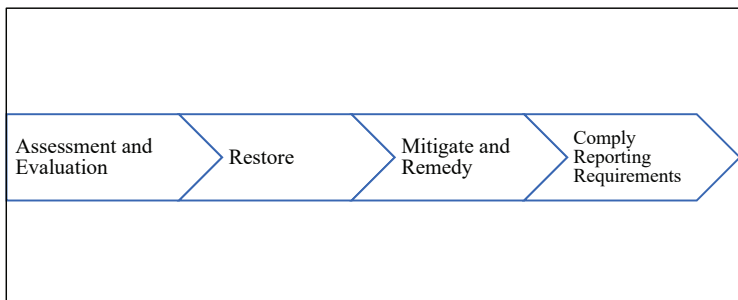


Figure 4. Security Incident Management Flow

The process flow above shall be executed as follows by the BRT in coordination with the PCOs:

Step 1: Assessment and Evaluation - all reported possible personal data and security breach and threats shall be assessed by the BRT for legitimacy and accuracy.

Step 2: Restore - once legitimacy of the incidents is confirmed, the BRT shall deploy all available resources and protocols to restore all affected databases and networks, if any. All personal data and information published physically accessed by unauthorized groups/individuals or stolen, must be immediately reported to the BRT for proper endorsement to law enforcement offices. Involved systems and physical files must be reported to the BRT for inventory and submission to the CT for proper documentation and reporting.

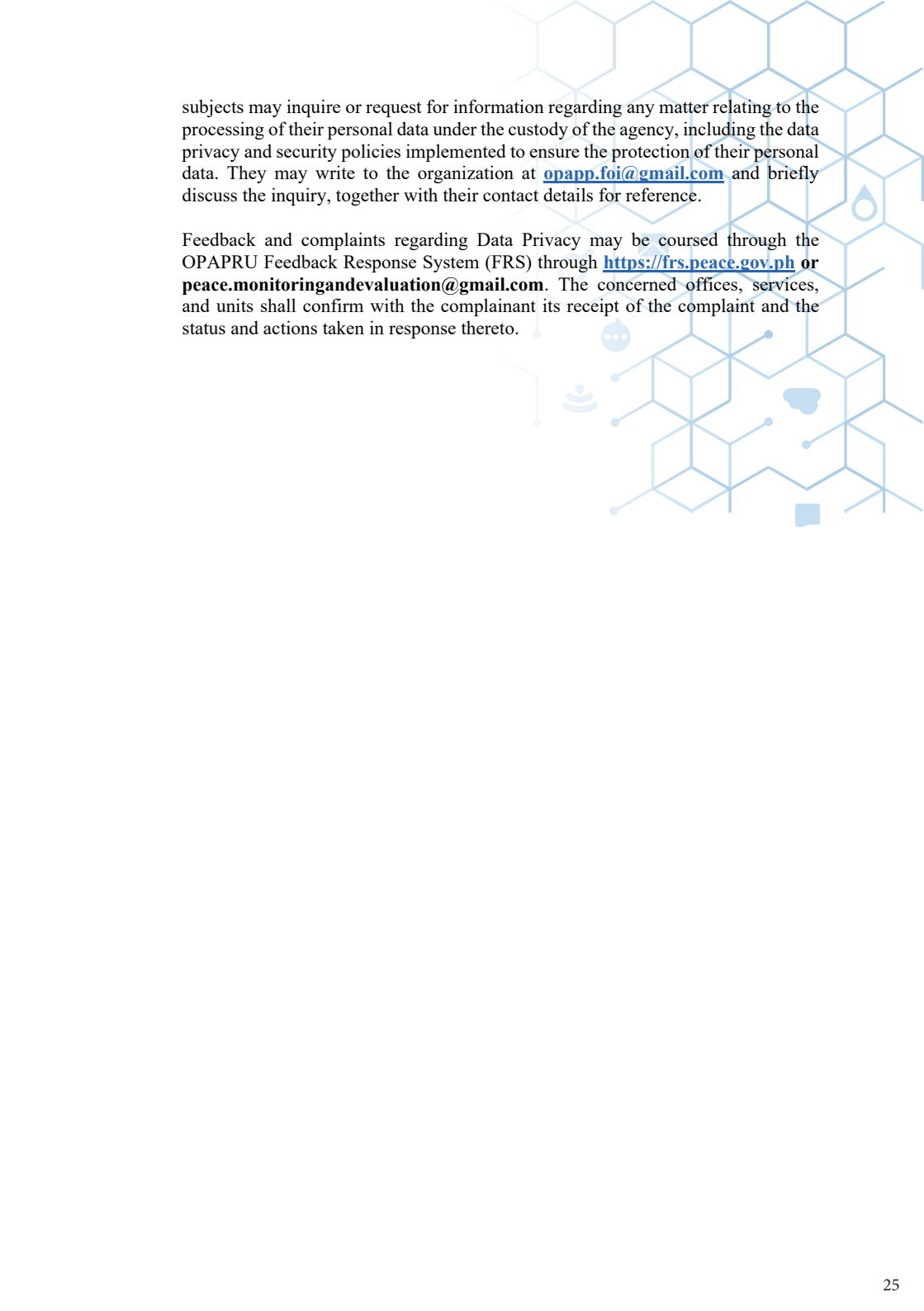
Step 3: Mitigate and Remedy - all affected systems, networks, database, and physical storage areas must be restored to its functional state by retrieval and restoration of digital and physical files. All unsecured systems, databases, and platforms shall be restricted until all security measures are fixed.

Step 4: Comply Reporting Requirements - using the Privacy and Security Incidents and Breaches Reporting Structure, the Breach Response Team, in collaboration with the concerned PCOs 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 OPAPRU 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**).

IX. INQUIRIES AND COMPLAINTS

All OPAPRU 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"*, OPAPRU 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 OPAPRU Feedback Response System (FRS) through <https://frs.peace.gov.ph> or peace.monitoringandevaluation@gmail.com. The concerned offices, services, and units shall confirm with the complainant its receipt of the complaint and the status and actions taken in response thereto.

LIST OF ANNEXES

ANNEX A	OPAPRU 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

OPAPRU DATA PRIVACY NOTICE

The Office of the Presidential Adviser on Peace, Reconciliation and Unity (OPAPRU), mandated to oversee, coordinate, and integrate the implementation of the comprehensive peace process, is committed to continuously uphold the right to privacy of all OPAPRU 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 on the purpose and legal basis for the processing of personal data and information collected from OPAPRU data subjects. This document shall also explain the security measures being adopted by the agency to protect the right to privacy, and effectively implement programs, projects, and activities in accordance to its mandates.

OPAPRU SERVICES

In accordance to its mandates, OPAPRU generally provides interventions and carries out functions to achieve the following objectives:

1. *Embedding Peace, Reconciliation and Unity in the Social Fabric.* There shall be direct and meaningful engagements with the rebel groups and the affected communities at the grassroots level in order to reach a peaceful settlement, and achieve a more permanent resolution to conflict. Peacebuilding initiatives shall: 1) address the legal status and security of former rebels; 2) ensure the protection of non-combatants and reduce the impact of the armed conflict in affected communities; and, 3) provide for community-based assistance services that cater to the economic, social, and psychological rehabilitation needs of former rebels, demobilized combatants, and civilian victims of the armed conflict, especially women and children;
2. *Enhancing Resilience for Peace.* Peace agreements shall be strictly implemented, and the enabling environment necessary to realize their goals shall be actively pursued. Peace advocacy and peace education programs, and the implementation of various confidence-building, healing and reconciliation measures to improve relationships of trust within divided and broken communities, between citizens and their government institutions, will be at the core of peacebuilding strategies, and;

3. *Social, Economic, and Political Reengineering.* There shall be government initiatives and mobilization of different sectors of society in addressing the root causes of internal armed conflicts and social unrest through the passage and implementation of key social, economic, and political reforms requiring administrative action, and new legislation of constitutional amendments.

PERSONAL INFORMATION COLLECTED AND METHODS OF COLLECTION

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

- Name
- Age
- Sex
- Gender
- Address
- Contact number
- Email address
- Agency/Organization of Affiliation
- Official Designation
- Personal Photo

The collection methods for these types of personal data and information include personal data sheets, online registration and survey forms, report submissions, and other authorized methods, and are collected by OPAPRU personnel and officials for appropriate purposes.

PURPOSES AND TIMING OF PROCESSING PERSONAL DATA AND INFORMATION

The OPAPRU 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 158, s. 2021.
2. Protection of privacy rights and welfare of OPAPRU 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, OPAPRU 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 OPAPRU offices, service, and units, including administrative and technical operations, among others;
3. Management of human resources, including external sources of technical service providers and prospective human resources;
4. External and internal affairs and relations;
5. Database and Records keeping and maintenance,
6. Documentations and Feedback;
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.

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

STORAGE, 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:

Format	Storage Type and Location	Retention	Disposal
Physical/Paper-based	Filing cabinets, water-proof, file folders, binders, file cases, laterals, etc. within OPAPRU building/ premises.	As necessary, as prescribed by R.A. 9470 or the National Archives of the Philippines (NAP) Act of 2007 (See Annex F for the NAP Circular 2: Prescribed retention periods for each specific record) , as authorized by OPAPRU officials	Upon authorization of relevant OPAPRU officials, or upon reaching the prescribed retention period of NAP, through shredding and incineration.
Electronic/Digital	OPAPRU servers, Agency-managed online storage, Agency-issued storage device		Upon authorization of relevant OPAPRU officials, or upon reaching the prescribed retention period of NAP, through device reformatting, complete manual and remote deletion.

The scanned copies of all physical/paper-based files must be secured for backup, these duplicates shall then be stored in authorized storage facilities and devices for digital copies. In all of the storage types and locations, appropriate labels must be indicated for ease of retrieval and tracking. 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 OPAPRU shall be accompanied with appropriate data sharing agreements.

RIGHTS OF OPAPRU DATA SUBJECTS

Pursuant to the RA 10173 Data Privacy Act of 2012 and its Implementing Rules and Regulations, all OPAPRU 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, OPAPRU 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 peacemonitoringandevaluation@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:	
<i>(Indicate which data from <u>Office</u>, <u>Service</u> and <u>Unit</u> being requested, include inclusive dates, focus area, etc.)</i>	
Data Format	<input type="checkbox"/> PDF <input type="checkbox"/> Excel <input type="checkbox"/> Word <input type="checkbox"/> Physical Others: _____
<i>(Tick appropriate box)</i>	

<p>Purpose of Data and Information Requested</p> <p>(Indicate nature of program/project/activity the data and information are being used in, inclusive dates)</p>	
<p>List of Personnel who will gain Data and Information Access</p> <p><i>Name/s</i></p> <p><i>Position/s</i></p> <p><i>Department/s/Division/s/Unit/s</i></p> <p><i>Contact Number/s</i></p> <p><i>Email address/s</i></p> <p><i>(use a separate sheet if necessary)</i></p>	

The Requesting Party agrees that OPAPRU 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 any form, for any purpose and in any manner whatsoever. To this end, the Requesting Party will provide OPAPRU 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)

Yes

No

NAME AND SIGNATURE OF AUTHORIZED REPRESENTATIVE

Requesting Party

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

RECEIVED AND PROCESSED BY:	APPROVED/ DISAPPROVED BY:
<hr/> <p>NAME AND SIGNATURE OF OPAPRU PERSONNEL OFFICE/SERVICE/UNIT</p>	<hr/> <hr/> <p>NAME AND SIGNATURE OF THE HEAD OFFICE/SERVICE/UNIT</p>

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 PEACE, RECONCILIATION AND UNITY (OPAPRU) 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.
 - 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 OPAPRU 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 PEACE, RECONCILIATION AND UNITY	PERSONAL INFORMATION REQUESTER
NAME OF THE HEAD OF THE AGENCY/AUTHORIZED OFFICIAL/PERSONNEL	NAME OF REPRESENTATIVE
Designation	Designation

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

NON-DISCLOSURE AGREEMENT

The **OFFICE OF THE PRESIDENTIAL ADVISER PEACE, RECONCILIATION AND UNITY**, herein referred to as “OPAPRU”, the undersigned employee hereby agrees and acknowledges:

1. That during the course of my employ there may be disclosed to me certain information from OPAPRU; 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 OPAPRU 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 OPARU, use for myself, or disclose or divulge to others including future employees, any trade secrets, confidential information, or any other proprietary data of OPAPRU in violation of this agreement.
3. That upon the termination of my employment from OPAPRU:
 - a. I shall return to OPAPRU 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 OPAPRU’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. OPAPRU 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 OPAPRU, its successors and assigns.

Signed this _____ day of _____, 202X.

NAME AND SIGNATURE OF EMPLOYEE
POSITION AND OFFICE/SERVICE/UNIT OF ASSIGNMENT

ANNEX D1
NON-DISCLOSURE AGREEMENT TEMPLATE FOR
CONSULTANTS

NON-DISCLOSURE AGREEMENT

The **OFFICE OF THE PRESIDENTIAL ADVISER ON PEACE, RECONCILIATION AND UNITY**, herein referred to as “OPAPRU” 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 OPAPRU 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 OPAPRU 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 OPAPRU, use for myself, or disclose or divulge to others including future employees, any trade secrets, confidential information, or any other proprietary data of OPAPRU in violation of this agreement.
3. That upon the termination of my contract with OPAPRU:
 - a. I shall return to OPAPRU 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 OPAPRU’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. OPAPRU 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 OPAPRU, its successors and assigns.

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

OFFICE OF THE PRESIDENTIAL ADVISER ON PEACE, RECONCILIATION AND UNITY	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 PEACE, RECONCILIATION AND UNITY (OPAPRU)**, are committed to achieving just and lasting peace through the Philippine Comprehensive Peace Process, as mandated by Executive Order No. 158, s. 2021, while implementing safeguards to protect your privacy and keep your personal data safe and secure.

Processing of Personal Data and Information

The OPAPRU 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

The OPAPRU shall implement reasonable and appropriate organizational, physical, and technical security measures for the protection of personal data that 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

The OPAPRU employees shall operate and hold personal data under strict confidentiality. They are required to sign non-disclosure agreements and 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;
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.

Contact Information

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

Contact Number: _____

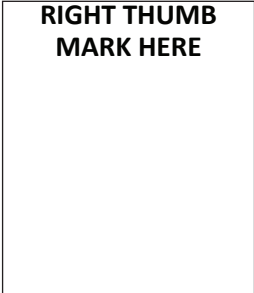
Email Address: _____

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



Date

Witness:

Signature Over Printed Name
Date

ANNEX E1

ASSENT FORM

For OPAPRU programs, projects and activities involving children (younger than 18 years old), an assent form must be administered by an OPAPRU 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 OPAPRU 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: _____

NAME AND SIGNATURE OF OPAPRU 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 PEACE, RECONCILIATION AND UNITY (OPAPRU)**.

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

DATE

SIGNATURE OVER PRINTED NAME OF OPAPRU REPRESENTATIVE

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	PERMANENT
	Issued by or for the head of agency reflecting routinary information or instruction	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 Deposits and Trust Funds General Collections Sub-Vouchers	5 years 5 years 5 years 2 years
48	Advices Checks Issued & Cancelled Remittance	4 years 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 Overtime Purchase of Equipment/Property Transfer of Fund Travel Others	1 year after expired
53	Bank Slips Deposits Remittances	10 years
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	<p>Reports</p> <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 	<p>10 years provided post-audited, finally settled and not involved in any case</p> <p>3 years</p> <p>10 years</p> <p>10 years</p> <p>5 years after case had been settled or terminated</p> <p>10 years provided post-audited, finally settled and not involved in any case</p>
83	Schedules of Accounts Receivables	3 years
84	<p>Statements</p> <ul style="list-style-type: none"> Accounts <ul style="list-style-type: none"> Current Payable Receivable Common Funds Financial Conditions Profits and Losses Reconciliations 	<p>3 years</p> <p>10 years</p> <p>PERMANENT</p> <p>10 years</p> <p>10 years</p> <p>PERMANENT</p> <p>10 years</p>
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	<p>Trial Balances and Supporting Schedules</p> <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 	<p>PERMANENT</p> <p>10 years after Annual Financial Report had been published</p> <p>PERMANENT</p> <p>10 years after Annual Financial Report had been published</p> <p>2 years after consolidated in the Annual Financial Report</p> <p>10 years after Annual Financial Report had been published</p> <p>PERMANENT</p> <p>10 years after Annual Financial Report had been published</p>

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 <u>HUMAN RESOURCE/PERSONNEL MANAGEMENT RECORDS</u>	4 years after superseded
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

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

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

How Security Incidents Occurred

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

Personal Data Breaches

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

PREPARED BY : _____

E-MAIL: _____

DESIGNATION : _____

CONTACT NO. : _____

DATE : _____

ANNEX G¹

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"

