Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
OFFICE OF THE SECRETARY
Bonifacio Drive, Port Area, Manila

BAGONG PILIPINAS

097.13 DPWH
05.28.2025

MAY 26 2025

DEPARTMENT ORDER)
)
NO. 94)
Series of 2025)

dN 5/28/2025

SUBJECT: Issuance of the DPWH Data Privacy Manual

To ensure the effective implementation of Republic Act No. 10173, otherwise known as the Data Privacy Act (DPA) of 2012, together with its Implementing Rules and Regulations and other relevant issuances from the National Privacy Commission (NPC), the DPWH Data Privacy Manual is hereby issued.

This Manual applies to all DPWH personnel, offices, divisions, and units involved in the collection, processing, storage, and sharing of personal data, including sensitive personal information, in the performance of their official duties and operations.

The primary objectives of the Data Privacy Manual are to:

1. Establish a cohesive framework for data privacy and protection within the DPWH;
2. Provide comprehensive guidelines for the lawful processing of personal data;
3. Ensure full compliance with the Data Privacy Act and all applicable regulations; and
4. Foster awareness and accountability among DPWH personnel regarding their data privacy responsibilities.

The Data Privacy Committee and the Technical Working Group shall review and update the Manual annually or as necessary to reflect amendments in relevant laws, regulations, or changes in DPWH operations.

All DPWH personnel are required to familiarize themselves with the Data Privacy Manual and comply with its provisions.

This Order supersedes Department Order No. 133, Series of 2023, and shall take effect immediately.

MANUEL M. BONOAN
Secretary

11.1.1 RBC/MSV

Department of Public Works and Highways
Office of the Secretary
WIN5P01864

DPWH DATA PRIVACY MANUAL

2025

Table of Contents

1 INTRODUCTION

The Department of Public Works and Highways (DPWH) is committed to protecting the personal data of individuals in accordance with the provisions of Republic Act No. 10173, also known as the Data Privacy Act of 2012. As a government agency that collects and processes personal data in the performance of its mandate, DPWH acknowledges its responsibility to implement appropriate safeguards to ensure the privacy, confidentiality, integrity, and availability of such data.

This Data Privacy Manual serves as a comprehensive guide for DPWH personnel and third-party service providers in understanding their roles and responsibilities regarding data privacy. It outlines the policies, practices, and procedures for lawful and secure data processing, from collection to disposal, and supports DPWH's efforts to maintain public trust and compliance with legal obligations.

By institutionalizing data privacy practices, DPWH aims to foster a culture of accountability, transparency, and respect for individual rights in all its programs, projects, and services.

2 LEGAL BASIS

This Manual is based on the following laws, rules, and regulations governing data privacy in the Philippines:

- Republic Act No. 10173 (Data Privacy Act of 2012) - Establishes the legal framework for data protection in the Philippines, mandating that public and private entities be responsible for collecting and processing personal data.
- Implementing Rules and Regulations (IRR) of RA 10173 - Provides detailed provisions for applying the Data Privacy Act, including guidelines on data subject rights, lawful processing, and accountability measures.
- National Privacy Commission (NPC) Circulars and Advisories Official - issuances from the NPC that clarify and interpret provisions of the law, recommend best practices and guide compliance efforts.
- Relevant Philippine Laws and Administrative Orders - Includes, but is not limited to:
    - ✓ Civil Service Commission (CSC) guidelines on employee records
    - ✓ Anti-Red Tape Act (ARTA)
    - ✓ Government procurement and e-Government regulations
    - ✓ Freedom of Information (FOI) Order and related policies

3 OBJECTIVES

The Data Privacy Manual has been developed to support the DPWH in upholding data subjects' rights and promoting responsible data governance across the agency. Its primary objectives are:

- Ensure the lawful processing of personal data within all levels and units of DPWH in accordance with applicable laws and regulations.
- Establish appropriate organizational, physical, and technical security measures that protect personal data from unauthorized access, alteration, disclosure, and destruction.
- Promote transparency and accountability by providing clear policies, responsibilities, and data privacy and security procedures.

- Strengthen public trust and confidence in the DPWH's delivery of infrastructure programs and services by demonstrating a commitment to ethical and compliant data management.

4 SCOPE AND COVERAGE

This Manual applies to all personal data processing activities conducted by the DPWH, whether through automated or manual systems, and across all organizational levels—including the Central Office (CO), Regional Offices (ROs), Unified Project Management Offices (UPMOs), and District Engineering Offices (DEOs). It shall also apply to all systems, tools, platforms, forms, and processes involved in the collection, use, sharing, storage, and disposal of personal data and shall be enforced throughout the entire data-processing lifecycle to protect personal information.

Covered entities and individuals include:

- Employees and job applicants whose personal and sensitive information is collected and processed during recruitment, employment, and human resource management.
- Contractors, consultants, suppliers, project proponents and third-party service providers who submit or gain access to personal data in connection with project implementation, procurement, or service delivery.
- Individuals who interact with DPWH through both online and offline channels, such as oversight agencies, Non-Government Agencies (NGAs), Local Government Units (LGUs), Government-Owned Controlled Corporations (GOCCs), stakeholders, clients, or members of the public submitting inquiries, requests, complaints, or feedback.

5 DEFINITION OF TERMS

To promote a common understanding across the agency, this section defines key terms used in this Manual. These definitions are based on the Data Privacy Act of 2012 and relevant issuances by the NPC:

- **Data Privacy Act of 2012 Alias DPA** – The Republic Act No. 10173, an Act protecting individual Personal Information in Information and Communications Systems in the government and the private sector, creating for this purpose a National Privacy Commission, and for other purposes.
- **Data Protection Officer Alias DPO** – An individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission: provided, that a government agency or private entity may have more than one DPO.
- **Data Subject** – An individual whose personal, sensitive personal, or privileged information is processed.
- **Personal Information Controller (PIC)** – A natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf.
- **Personal Information Processor (PIP)** – Any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.
- **Compliance Officer for Privacy Alias COP** – An individual or individuals who shall perform some of the functions of a DPO.

- **Data Breach Response Team** – The group responsible for managing security incidents and data breaches, enforcing incident response policies, ensuring compliance with data protection laws, and taking prompt action to assess, mitigate, and report breaches while restoring system integrity.
- **Head of Office** – The highest ranking official in the office, i.e., Bureau Director, Service Director, Regional Director, Cluster/Project Director, District Engineer.
- **Personal Information** – Any data, whether recorded in material form or not, from which an individual's identity is apparent or can be reasonably and directly ascertained, or when combined with other data, would identify an individual.
- **Sensitive Personal Information (SPI)** – A personal information about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations; details about an individual's health, education, genetic or sexual life, or any proceeding for any offense committed or alleged to have been committed by such individual, including the outcome of such proceedings or the sentence of any court; information issued by government agencies that is unique to an individual, such as social security numbers, health records (past or present), licenses or their denial, suspension, or revocation, and tax returns; and any data specifically classified as confidential by an executive order or an act of Congress.
- **Consent** – A freely given and informed agreement to collect and process personal data.
- **Privacy Impact Assessment (PIA)** – A process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure.
- **Data Sharing Agreement (DSA)** – A contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the personal information controllers involved in the transfer of personal data between or among them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the data subjects: provided, that only personal information controllers should be made parties to a data sharing agreement.
- **Personal Data Breach** – A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
- **Project Affected Person (PAP)** - any individual, household, business, or institution—public or private—who will suffer partial or total loss of land, structures, improvements, or livelihood due to right-of-way acquisition for an infrastructure project.

6 ROLES AND RESPONSIBILITIES

The effective implementation of the Department's Data Privacy Program relies on defining key offices and personnel roles and responsibilities. This section outlines the individuals and organizational units tasked with overseeing, managing, and supporting personal data protection within the Department.

6.1 Personal Information Controller (PIC)

The Secretary is the PIC in DPWH. The PIC is ultimately responsible for ensuring the protection of all personal information and that processing such personal information is in line with the provisions of the DPA.

6.2 Data Protection Officer (DPO)

The Chairperson of the Data Privacy Committee shall be designated as the DPO. The DPO shall implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, or alteration.

6.3 Data Privacy Committee (DPC)

The DPC shall include the following:

Chairperson:
Undersecretary for Support Services
Vice Chairperson:
Assistant Secretary for Support Services
Members:
Director, Stakeholders Relations Service (SRS)
Director, Legal Service (LS)
Director, Human Resource and Administrative Service (HRAS)
Director, Information Management Service (IMS)
Director, Finance Service (FS)
Director, Bureau of Quality and Safety (BQS)
Director, Bureau of Research and Standards (BRS)
Director, Procurement Service (PrS)

The Committee shall be responsible for recommending programs with regard to RA 10173. The following are the duties and responsibilities of the DPO and its Committee:

1. Monitor the compliance with the DPA, its IRR, issuances by the NPC, and other applicable laws and policies;
2. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC and
3. Advise the PIC regarding complaints and/or exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification, or deletion of personal data).
4. Serve as the contact person of the NPC and other authorities in all matters concerning data privacy and security.

6.4 Technical Working Group (TWG)

The TWG shall provide support to the DPC in the execution of the Department's data privacy program. This includes the following functions:

1. Conduct and maintain an inventory of all data. containing Personal and Sensitive Information.
2. Ensure the conduct of PIA to identify risks in data processing systems.
3. Assist in the drafting of the Data Privacy Management Program.
4. Assist in drafting the Data Privacy Manual and other documentary requirements to ensure the implementation of measures and procedures that will guarantee the safety and security of personal data under its control or custody.
5. Conduct data privacy awareness campaigns and training sessions for the Department.

6. Submit reports, such as Annual Reports, Data Breach Reports, etc., to the NPC.
7. Keep up-to-date with Data Privacy laws and issuances to ensure the Department adheres to the DPA.

6.5 Compliance Officers for Privacy (COP) and Data Breach Response Team (DBRT)

The COP shall be designated in the Central Office, Regional, and District Engineering Offices. They shall also be designated the Team Lead of the Data Breach Response Team to monitor compliance with applicable laws and regulations to protect data privacy and security in their respective areas of concern. The Data Breach Response Team shall be constituted with the following:

	Central Office (Bureaus/Services/UPMO Clusters)	**Regional Office**	**District Engineering Office**
Team Lead	Director, Legal Service	Regional Directors, Chief of Legal Division	District Engineers, Chief of Administrative Section
Members	Directors and Designated Administrative Officers of the Bureaus, Services and UPMO Clusters	Chief of Administrative Division, Regional Information Technology Support Officer (RITSO), Regional Public Information Officer	District Information Technology Support Officer (DITSO), Designated Public Information Officer

The COPs shall report to the DPO for all matters relating to Data Privacy in their respective Offices and shall perform the following duties and responsibilities:

- Ensure proper data breach and security incident management, including the preparation and submission of reports to the DPC and other documentation concerning security incidents or data breaches within the prescribed period;
- Inform and cultivate awareness of privacy and data protection within the organization, including all relevant laws, rules, regulations, and issuances of the NPC;
- Advocate for the development, review and/or revision of policies, guidelines, projects, and/or programs relating to privacy and data protection by adopting a privacy-by-design approach;
- Serve as the contact person of data subjects and the DPC in all matters concerning data privacy or security issues or concerns;
- Cooperate, coordinate, and seek the DPC's advice on data privacy and security; and
- Perform other duties and tasks that the DPC may assign that will further the interest of data privacy and security and uphold the rights of the data subjects.

6.6 Data Breach Response Team (DBRT)

In the event of a data breach or cyber incident involving government digital assets, the DBRT shall coordinate with the DPWH Government Computer Emergency Response Team (GCERT) for the immediate containment, thorough investigation, and effective remediation of the incident.

6.7 Director of Human Resource and Administrative Service (HRAS)

The HRAS Director shall ensure that all personnel—both new hires and existing employees—are adequately informed and trained on the data privacy policies, standards, and procedures of the Department, including the implementation of physical security measures in accordance with the DPA.

Specifically, the HRAS Director shall:

- Ensure that all employees undergo mandatory orientation and periodic training on the DPA, its IRR, and relevant DPWH data privacy policies;
- Ensure that training materials are updated regularly in coordination with the DPO to reflect current laws, best practices, and agency-specific guidelines;
- Ensure that all employees sign a document confirming they have received, understood, and will follow DPWH's Data Privacy policies and procedures;
- Ensure that personnel records related to data privacy training and acknowledgments are securely maintained and accessible for compliance verification purposes;
- Oversee the implementation and monitoring of physical security measures—such as CCTV systems, access control, and visitor management—to safeguard personal data within DPWH premises;
- Coordinate with the DPO to conduct PIA for existing and new physical security systems, ensuring alignment with data protection standards.

6.8 Director of Legal Service (LS)

The LS Director shall be responsible for the legal review and evaluation of data privacy-related documents and instruments to ensure compliance with the DPA, its IRR, and relevant issuances and advisories of the NPC.

Specifically, the LS Director shall:

- Ensure that the contents and provisions of the Data Privacy Manual are consistent with the requirements of the DPA and do not contradict the provisions of the Freedom of Information (FOI) Program.
- Provide legal advice and guidance on data privacy, confidentiality, and disclosure in coordination with the DPO and the DPC.

6.9 Director of Information Management Service (IMS)

The IMS Director shall ensure that all applications and systems are planned, designed, and implemented in accordance with the DPWH Data Privacy policies and procedures.

Specifically, the IMS Director shall:

- Ensure that all IT systems, including desktop, web-based, and mobile platforms, incorporate privacy-by-design and privacy-by-default principles from planning to deployment stages;
- Ensure that all IT systems comply with applicable privacy, security, and data protection standards issued by the NPC;
- Oversee the implementation of IT security controls, such as encryption, user authentication, access restrictions, and system audits;
- Oversee the management of backups and disaster recovery mechanisms to maintain the availability, integrity, and confidentiality of personal data;
- Ensure that the PIA are conducted for all new applications or existing applications undergoing major enhancements that process personal data;
- Ensure coordination with the DPO to address privacy risks related to IT infrastructure and services.

7 PROCESSING OF PERSONAL INFORMATION

7.1 Collection

The Department collects basic personal data from its personnel, contractors, consultants, suppliers, and other external stakeholders. This includes but is not limited to full names, addresses, email addresses, contact numbers, and details of their services, where applicable.

Personal information is processed in the context of various operational and administrative activities. Examples include employee management, contract implementation, accreditation of contractors, consultants, and suppliers, feedback management, stakeholder and community consultations, Right-of-Way (RoW) acquisition, and relocating affected individuals before project implementation. These activities are carried out across different offices and systems, involving multiple personnel and data handlers.

DPWH processes personal information in accordance with the core principles outlined in the DPA: transparency, legitimate purpose, and proportionality. This means that:

- **Transparency**: Data subjects must be fully informed about how their personal data will be processed—its nature, purpose, and scope. They should understand the risks and safeguards involved, be able to identify the personal information controller, know their rights under the law, and be guided on how to exercise these rights. All data privacy communications should be clear, accessible, and written in plain language.
- **Legitimate Purpose**: The collection and use of personal data must serve a lawful, specific, and clearly stated purpose. It must be in accordance with existing laws, public morals, or public Policy.
- **Proportionality**: The processing of personal data must be appropriate, relevant, and limited to what is necessary to achieve the stated purpose. Personal data should not be collected or retained if the intended objective can be reasonably accomplished through other less intrusive means.

For DPWH website visitors, a Data Privacy Notice for Website (Annex A) is provided to ensure transparency on how personal data is collected, used, and protected when accessing or interacting with the Department's online platforms.

For other data collection processes that involve personal information, a DPWH Data Privacy Notice and Consent Form (Annex B) shall be filled out to collect personal data from all relevant stakeholders.

7.2 Use

Personal information shall be used strictly for the declared and legitimate purposes for which it was collected. The use shall be limited to what is necessary to perform the official functions and responsibilities of the Department.

All personnel handling data (PIPs) are accountable for maintaining the confidentiality, integrity, and lawful processing of data per DPWH's privacy policies.

7.3 Disclosure and Sharing

All personnel shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, retirement, or end of other contractual relations. To reinforce this obligation, all personnel handling personal and sensitive personal information shall be required to sign a Non-Disclosure Agreement (NDA) (see Annex C) as a condition of their engagement. Personal information under the custody of the DPWH shall be disclosed only according to a lawful purpose and authorized recipients of such data.

For data sharing between agencies, a Data Sharing Agreement (DSA) (See Annex D) shall be signed by both parties. It must comply with the conditions under the Data Sharing Agreements Involving Government Agencies of NPC. The Legal Service shall properly review all DSA's to check if the content and provisions comply with the DPA, its IRR, and relevant NPC issuances.

7.4 Storage

Personal information, whether electronic or print, shall be protected against accidental or unlawful destruction, deletion, alteration, disclosure, or other unlawful processing.

The Department shall implement appropriate security measures to store collected personal information, depending on the nature of the data.

7.5 Retention and Disposition Procedure

All personal information gathered shall not be retained longer than specified in the Records Disposition Schedule (RDS).

After the specified period, all physical and electronic copies of personal information shall be disposed of and destroyed through secured means following the rules and issuances of the National Archives of the Philippines (NAP).

7.6 Access

The Department shall strictly regulate access to personal data under its control or custody. Only authorized personnel and relevant stakeholders of the Department shall be allowed to access such personal data for any purpose except those contrary to law, public policy, public order, or morals.

The IMS shall manage and provide secured access to the Department's applications and software systems with the approval of the Application/System Owners. Access to all electronic and physical documents containing personal information shall be subjected to the approval of the concerned Head of Office.

8 SECURITY MEASURES

8.1 Organizational Measures

8.1.1 Conduct of Privacy Impact Assessment (PIA)

DPWH shall conduct a PIA (see Annex E) relative to all activities, projects, and systems involving the processing of personal data. It shall be undertaken for every new and existing process and system involving personal data. It should follow the NPC's Guidelines on Privacy Impact Assessment.

8.1.2 Conduct of Training or Seminars

a. DPWH Employees

All personnel of the Department, regardless of employment status or tenure, are required to follow the DPA and the Department's data privacy policies and procedures.

Upon onboarding, all personnel shall sign an acknowledgment form confirming that they are aware of the DPA and understand their roles and responsibilities in protecting personal data.

The HRAS and their Regional and District counterparts, in coordination with the DPC and TWG, shall ensure that all personnel receive appropriate Data Privacy awareness training.

All personnel acting as Personal Information Processors (PIPs) must undergo regular training on data privacy principles, physical security protocols, and handling personal and sensitive information properly. These training sessions will be conducted periodically to reinforce compliance with data protection policies, address emerging security threats, and ensure that all processors understand their critical role in safeguarding personal data.

b. External Stakeholders

All contractors, consultants, and suppliers, including Project Affected Persons (PAPs), doing business with the Department, shall be made aware of the Department's data privacy policies and procedures at the commencement of any project or engagement.

They shall submit a duly accomplished DPWH Data Privacy Notice and Consent Form (Annex B), which shall be filed and maintained as part of the official project documentation.

8.1.3 Documentation of Data Privacy-related activities

Detailed and accurate documentation of all department activities, projects, and processing systems shall be carried out by the Department DPO, DPC, COPs and the TWG.

8.1.4 Review of Privacy Manual

The Department shall regularly review and update its privacy and security policies to ensure alignment with evolving data privacy laws, regulations, and best practices.

8.2 Physical Measures

8.2.1 Access Control

Paper-based personal records must be securely stored, with access restricted to authorized personnel only. Similarly, data centers, including server rooms, backup rooms, and records storage areas, should be accessible only to authorized individuals. The Head of Office is responsible for maintaining an updated list of authorized personnel permitted access to these secure areas.

8.2.2 Access Procedures for DPWH Personnel

Access to personal information related to current and former DPWH personnel, including applicants' records, is restricted to their respective COPs, Heads of Offices, and the Chief Administrative Officer of Bureaus, Services, Project Management Offices, Regional Offices, and District Engineering Offices.

To access their 201 File, personnel must fill out the Personal Data Request for Action Form (Annex F) and get approval from the Head of Office. Once approved, the respective Administrative Officer will get the needed records, make copies, and give them to the requesting personnel.

At no time should authorized personnel bring electronic devices, storage media, or any other unauthorized equipment when accessing personal files or records of DPWH personnel, applicants, or stakeholders.

8.2.3 Monitoring and Logging of Access

All authorized personnel who access stored personal information must record the date, time, duration, and purpose of each access in a designated logbook.

8.2.4 Visitor Policy

Visitors to areas where personal or sensitive data is processed or stored must follow strict procedures. They must be logged upon entry, issued a visitor badge, and escorted at all times by authorized personnel. Visitors are not permitted to access restricted areas unless accompanied by authorized personnel. The duration of the visit and areas of access will be limited based on necessity, ensuring minimal exposure of personal or sensitive data.

8.3 Technical Measures

The IMS must implement technical security measures to ensure appropriate and sufficient safeguards to secure the processing of personal data, particularly the computer network in place, including encryption and authentication processes that control and limit access. They include the following, among others:

8.3.1 Monitor Security Breaches

a. Installation and Maintenance of Endpoint Security Software (anti-virus) – The Department shall install and maintain endpoint security software for all computers/workstations, laptops and servers connected to the network.
b. User Authentication – A User authentication shall be used when accessing the Department's ICT resources such as application systems, email, internet, etc.
c. Use of Intrusion Detection and Prevention System – An intrusion detection and prevention system shall monitor security breaches and alert the organization of any attempt to interrupt or disturb its IT systems.
d. Implementation of Network Firewall – A firewall shall secure the Department's network from unauthorized access to its data from external sources.
e. Report on technical security measures and information security tools in place – The IMS shall regularly analyze the firewall logs to monitor security breaches and alert the DPO of any suspected unauthorized access to the DPWH network.
f. Monthly security reports shall be generated from the firewall and endpoint security software.
g. Record of security incidents and personal data breaches, including notification for personal data breaches, shall be prepared in the event of security incidents and data breaches. Personal Data Security Breach Report Form (Annex G) shall be used for this purpose.

8.3.2 Security Features of the Software/s and Application/s Used

8.3.2.1 Review and Evaluation of Software Applications

All software applications—whether off-the-shelf or customized—must undergo review and evaluation before installation on any computer or device to ensure they comply with the Department's licensing, security and data privacy policies.

For existing software applications that process the personal information, the following procedures must be observed:

a. System Security Evaluation

In coordination with the respective Application User Coordinator, the IMS shall evaluate the application's security features, specifically its storage, backup, and recovery protocols.

If any protocol contradicts the data privacy principles outlined in the DPA, necessary corrective measures must be implemented immediately.

b. Privacy Compliance During Preventive Maintenance of ICT Equipment

During scheduled ICT preventive maintenance, the IMS and its counterpart

Regional and District IT Support Officers (ITSOs) shall inspect installed applications for compliance with the Department's data privacy policies.

If any application is found to pose a security risk or potentially disrupt network operations, the following steps shall be taken:

- IMS/ITSOs shall notify the concerned end-user
- The identified software shall be immediately uninstalled
- IMS/ITSO shall prepare and file a Preventive Maintenance Report for proper documentation and action

c. Regular Updating of Security Patches

The IMS and ITSOs shall ensure that all workstations and servers connected to the DPWH network are updated regularly with the latest security patches and updates.

8.3.3 Vulnerability Tests

IMS shall conduct regular vulnerability assessments of all critical hardware and software systems to ensure the continued effectiveness of its security measures. These assessments shall be carried out internally—within the DPWH's network—to simulate real-world attack scenarios that may target the Department's digital infrastructure. The scope of these assessments includes, but is not limited to, penetration testing, network vulnerability scans, application security reviews, and system configuration audits. This proactive approach helps identify potential security gaps and reinforces the department's readiness against emerging cyber threats.

8.3.4 Monitoring of Access for Personal Data

Access to DPWH ICT resources—including onsite, remote, and online systems—shall be granted upon submission of a formal request endorsed by the employee's Head of Office and approved by the IMS and must comply with the latest policy on the use of the Department's ICT resources.

8.3.5 Backup of Personal Data

Backup policies (e.g., ICT Data Backups, System backups, data recovery, etc.). The data from servers shall be regularly backed up and stored in a secured location, both onsite and off-site.

9 BREACH AND SECURITY INCIDENTS

This procedure outlines the steps to be taken in case of a suspected or confirmed personal data breach to ensure a timely response, containment, and compliance with regulatory requirements.

9.1 Identification and Reporting

- Any employee or third-party processor who suspects a data breach must immediately report the incident to the DPO or designated COPs.

- Reports should include the date/time of discovery, nature of the breach, affected systems/data, and initial observations.

9.2 Initial Assessment and Containment

The DPO/COPs, in coordination with the DBRT and GCERT (as necessary), shall conduct an initial assessment to:

- Verify if a breach has occurred.
- Identify the scope and nature of the breach (e.g., unauthorized access, accidental disclosure, loss, or destruction of data).
- Implement immediate containment measures to limit further exposure (e.g., isolating affected systems, changing credentials, revoking access).

9.3 Full Evaluation

Conduct a full risk assessment to determine:

- The type and sensitivity of the personal data involved.
- The number of affected data subjects.
- Possible consequences to individuals (e.g., identity theft, reputational harm).
- The root cause of the breach.

9.4 Breach Notification

- The DPO shall notify the NPC within 72 hours of knowledge of the breach using the prescribed Personal Data Security Breach Report Form (Annex G).
- Affected data subjects shall also be informed without undue delay, with clear instructions on how to mitigate risks.

9.5 Documentation and Reporting

- All data breach incidents shall be recorded by the Head TWG in the Data Breach Management Log (Annex H) including:
  - ✓ Timeline of events
  - ✓ Persons involved
  - ✓ Actions taken
  - ✓ Communications made
- Reports shall be reviewed by management for accountability and future prevention.

9.6 Remediation and Prevention

- Implement corrective actions to address vulnerabilities and prevent recurrence (e.g., policy updates, employee training, system upgrades).
- Review and update the Privacy Management Program, security controls, and incident response policies as necessary.

10 RIGHTS, INQUIRIES AND COMPLAINTS OF DATA SUBJECTS

10.1 Rights of Data Subjects

As provided under the DPA, data subjects have the following rights in connection with the processing of their personal information:

10.1.1 Right to be Informed

The data subject has the right to be informed that their personal data shall be, is being or has been processed.

The right to be informed is a fundamental right as it empowers the data subject to consider other actions to protect their data privacy and assert their other privacy rights.

10.1.2 Right to Access

Related to their right to be informed, the data subject also has a right to gain reasonable access to their personal data.

Access to the following can be requested:

- Contents of their personal data that were processed;
- Sources from which the data were obtained;
- Names and addresses of the recipients of their data;
- How the data was processed;
- Reasons for disclosure to recipients, if there were any;
- Information on automated processes where the data will or is likely to be made as the sole basis for any decision that would significantly affect them;
- Date when the data was last accessed and modified; and
- Name and address of the personal information controller.

10.1.3 Right to Object

The data subject has the right to object to the processing of their personal data, including paper-based processing, automated processing or profiling.

Likewise, the right to be notified and given an opportunity to withhold consent to the processing in case of any changes to the Information.

10.1.4 Right to Erasure or Blocking

Under the law, the data subject has the right to suspend, withdraw or order the blocking, removal or destruction of their personal data. This right can be exercised upon discovery and substantial proof of any of the following:

a. Their personal data is incomplete, outdated, false, or unlawfully obtained
b. It is being used for purposes not authorized;
c. The data is no longer necessary for the purposes for which they were collected;

d. Withdrawal of consent or objection to its processing, and there is no overriding legal ground for its processing;
e. The data concerns personal Information prejudicial to the data subject – unless justified by freedom of speech, of expression, or otherwise authorized;
f. The processing is unlawful; or
g. The personal information controller, or the personal information processor, violated their right as a data subject.

10.1.5 Right to Damages

The data subject may claim compensation if they suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of their personal data, considering any violation of their rights and freedoms as data subject.

10.1.6 Right to File a Complaint

If they are the subject of a privacy violation or personal data breach, or who are otherwise personally affected by a violation of a DPA, they may file complaints with the NPC.

10.1.7 Right to Rectification

The data subject has the right to dispute any inaccuracy or error in their personal data and have the personal information controller correct it immediately unless the request is vexatious or unreasonable. Once corrected, the PIC should ensure that the data subject has access to both new and retracted information and simultaneous receipt of the new and the retracted information by the intended recipients thereof.

10.1.8 Right to Data Portability

Where the personal information is processed by electronic means, the data subject has the right to obtain from the personal information controller a copy of their personal data, a copy of such data in an electronic or structured format that is commonly used and allows for further use.

This right aims to empower the data subject and give them more control over their personal data. This right is subject to certain conditions, supporting user choice, control, and employee empowerment.

It enables the free flow of personal information across organizations according to their preference. This is important, especially now that several organizations and services can reuse the same data.

Data portability allows personal data management and data transmission from one personal information controller to another. As such, it promotes competition that fosters better services to the public.

10.2 Inquiries and Complaints of Data Subject

For inquiries, correction or erasure requests, and complaints, data subjects may fill out the Personal Data Request for Action Form (see Annex F), available for download on the

DPWH website, and submit the completed form to the COP of the concerned office, either in person or via email.

The COP shall review and act on the request, ensuring that all concerns are addressed in accordance with the timelines and procedures prescribed under the DPA and the Department's internal policies.

After resolution, the COP shall submit a summary report of the concerns received, actions taken, and any unresolved matters to the DPO through the TWG for consolidation.

The TWG shall maintain a centralized log of all data privacy-related inquiries and complaints based on the consolidated reports from the COPs.

11 PENALTIES

A corresponding penalty under the DPA, as well as applicable DPWH policies and administrative rules, shall be imposed on any individual found responsible for violating data privacy protocols.

The table below outlines punishable acts and their corresponding penalties under the law:

Punishable Act	Jail Term	Fine
Access due to negligence	1 to 3 yrs; 3 to 6 yrs	₱500,000 to ₱4,000,000
Unauthorized processing	1 to 3 yrs; 3 to 6 yrs	₱500,000 to ₱4,000,000
Unauthorized purposes	18 mos to 5 yrs; 2 to 7 yrs	₱500,000 to ₱2,000,000
Improper disposal	6 mos to 2 yrs; 3 to 6 yrs	₱500,000 to ₱2,000,000
Intentional breach	1 to 3 yrs	₱500,000 to ₱2,000,000
Concealing a breach	18 mos to 5 yrs	₱500,000 to ₱2,000,000
Malicious disclosure	18 mos to 5 yrs	₱500,000 to ₱1,000,000
Unauthorized disclosure	1 to 3 yrs; 3 to 5 yrs	₱500,000 to ₱2,000,000
Combination of acts	3 to 6 yrs	₱1,000,000 to ₱5,000,000

12 REFERENCES

- NPC Advisory No. 2017-01 re Designation of Data Protection Officer
- NPC Privacy Tool Kit 3rd Edition – A Guide for Management & Data Protection Officer
- Department Order No. 9, Series of 2025 – Policies and Guidelines on the Use of DPWH Information and Communications Technology (ICT) Resources

13 LIST OF ANNEXES

A. Website Data Privacy Notice
B. Data Privacy Notice and Consent Form
C. Non-Disclosure Agreement
D. Data Sharing Agreement
E. Privacy Impact Assessment
F. Personal Data Request for Action Form
G. Personal Data Security Breach Report Form
H. Data Breach Management Log

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

WEBSITE DATA PRIVACY NOTICE

Last updated: [Insert Date]

What We Collect

When you browse our website, we may collect the following information:

- Basic browser details (type, version, IP address)
- Date and time of access
- Pages visited
- Information you voluntarily provide (e.g., through forms or email)

How We Use Your Data

The personal data we collect is used for:

- Improving website content and user experience
- Responding to inquiries or requests
- Processing data subject requests (e.g., access, correction, erasure)
- Monitoring website traffic and trends

Data Sharing and Storage

We do not sell or share your personal data with third parties unless:

- Required by law or authorized by a government authority
- Needed for official government functions or service delivery

All data is stored securely and retained only as long as necessary for stated purposes.

Use of Cookies

Our website may use cookies to enhance your browsing experience. You may choose to disable cookies through your browser settings, though some site functions may not work properly as a result.

Your Rights as a Data Subject

Under the Data Privacy Act of 2012, you have the right to:

- Right to be informed
- Right to object
- Right to access
- Right to correct
- Right to erasure or blocking
- Right to file a complaint
- Right to damages
- Right to data portability

To make a request, please fill out our *Personal Data Request for Action Form* and email it to dpo@dpwh.gov.ph.

Contact Us

For any questions or concerns regarding this Data Privacy Notice or your personal data, you may contact:

Undersecretary MARICHU A. PALAFOX
Data Protection Officer
Department of Public Works and Highways
Bonifacio Drive, Port Area, Manila, Philippines
Email: dpo@dpwh.gov.ph
Tel: +639 5304 3242

Annex B

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

DATA PRIVACY NOTICE AND CONSENT FORM

The Department of Public Works and Highways (DPWH) collect and process your personal data in accordance with the Data Privacy Act of 2012 and our organizational policies. The personal data we collect may include your name, contact information, and any other details relevant to our services. The data will only be processed for specific purposes related to the operation of *[Office Name]* and its services.

We take your privacy seriously and implement safeguards to protect your personal data from unauthorized access, disclosure, and misuse. These measures include secure systems, encryption, and strict access controls. However, all data processing involves inherent risks, and we strive to mitigate those risks through careful management and regular reviews of our processes.

You have the following rights under the law:

- Right to be informed
- Right to object
- Right to access
- Right to correct
- Right to erasure or blocking
- Right to file a complaint
- Right to damages
- Right to data portability

Our Data Protection Officer (DPO) can assist you with privacy-related inquiries, concerns, or requests. You may contact the DPO through the following:

Undersecretary MARICHU A. PALAFOX
Data Protection Officer
Department of Public Works and Highways
Bonifacio Drive, Port Area, Manila, Philippines
Email: dpo@dpwh.gov.ph
Tel: +63 5304 3242

Consent and Acknowledgement

I have read and understood this Data Privacy Notice. I voluntarily give my consent to the *[Office Name]* to collect, use, and process my personal data for *[process name]* in accordance with the Data Privacy Act of 2012.

Signature: _____
Printed Name: _____
Date: _____

Annex C

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE

NON-DISCLOSURE AGREEMENT

This Agreement is made and entered into on this ___ day of _____, 20___, by and between:

Department of Public Works and Highways (DPWH), with principal offices at Bonifacio Drive, Port Area, Manila, herein referred to as the 'Disclosing Party', and

[Name of Staff], of [Position/Division/Office], herein referred to as the 'Receiving Party'.

1. Purpose

The Receiving Party, in the performance of duties for or on behalf of DPWH, may have access to personal, sensitive, or privileged information. This Agreement aims to ensure that such information is kept confidential and protected.

2. Definition of Confidential and Personal Information

Confidential Information includes any data, documents, files, or other information, whether in written, digital, or verbal form, that is:

- Personal or sensitive in nature under the Data Privacy Act of 2012 (Republic Act No. 10173);
- Not publicly available;
- Shared for official duties or in confidence.

3. Obligations of the Receiving Party

The Receiving Party agrees to:

a. Keep all confidential and personal information strictly confidential;
b. Use such information only for official DPWH functions;
c. Not disclose, share, copy, or disseminate such information without proper authority;
d. Secure physical and electronic files containing sensitive information;
e. Report any breach or potential breach of confidentiality immediately.

4. Duration

This Agreement remains effective throughout the staff's employment or engagement with DPWH and shall continue to bind the Receiving Party even after separation, resignation, or transfer.

5. Breach and Liability

Any breach of this Agreement may result in administrative, civil, or criminal liability under applicable laws, including but not limited to the Data Privacy Act of 2012.

IN WITNESS WHEREOF, the parties have hereunto set their hands this ___ day of _____, 20___.

Department of Public Works and Highways (DPWH)

By: _____
Name: _____
Position: _____
Signature: _____
Date: _____

Receiving Party

By: _____
Name: _____
Position: _____
Signature: _____
Date: _____

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

DATA SHARING AGREEMENT

This Data Sharing Agreement ("Agreement") is entered into on this ___ day of _____, 20___, by and between:

The Department of Public Works and Highways (DPWH), with principal offices at Bonifacio Drive, Port Area, Manila, hereinafter referred to as the "First Party",

and

[Receiving Party], of [Position/Division/Office], hereinafter referred to as the "Second Party".

1. Purpose

This Agreement sets out the terms and conditions under which personal or sensitive information may be shared between the First Party and the Second Party, in accordance with Republic Act No. 10173 or the Data Privacy Act of 2012. This sharing aims to support the official duties and functions of DPWH.

2. Data to be Shared

The data to be shared includes, but is not limited to, names, contact information, addresses, and other relevant personal or sensitive information necessary to perform official functions.

3. Responsibilities of the Parties

Each Party agrees to:
a. Use the data only for legitimate, official purposes;
b. Ensure that the data is accurate, complete, and up to date;
c. Implement appropriate organizational, technical, and physical security measures to safeguard the data;
d. Notify the other party immediately in case of a data breach or unauthorized access.

4. Data Retention and Disposal

The data shall be retained only as long as necessary to fulfill the intended purpose and shall be securely destroyed or returned to the First Party once no longer needed.

5. Confidentiality

Both parties agree to maintain the confidentiality of the shared data and not to disclose it to any unauthorized person or entity.

6. Breach and Liability

Any unauthorized use or disclosure of data may result in administrative, civil, or criminal liability under applicable laws. The offending party shall be held liable for any damages resulting from such breach.

7. Amendment and Termination

This Agreement may be amended only in writing and signed by both parties. It may be terminated by either party upon written notice, subject to proper data disposition procedures.

8. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the Republic of the Philippines, particularly the Data Privacy Act of 2012.

IN WITNESS WHEREOF, the parties have hereunto set their hands this ___ day of _____, 20___.

Department of Public Works and Highways (DPWH)

By: _____
Name: _____
Position: _____
Signature: _____
Date: _____

Receiving Party

By: _____
Name: _____
Position: _____
Signature: _____
Date: _____

Annex E

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

PRIVACY IMPACT ASSESSMENT

This Privacy Impact Assessment (PIA) is intended to help assess the privacy risks associated with data processing activities within the Department of Public Works and Highways (DPWH). The form must be completed for any project or process involving the collection, use, storage, or sharing of personal information.

Project/Process Information

a. Name of the Project/Process: _____
b. Project/Process Description: _____
c. Department/Unit Handling the Project/Process: _____
d. Date of Assessment: _____
e. Contact Person (Name, Position, Contact Info): _____

Data Information

a. Type of Data Collected (Personal, Sensitive, etc.):_____
b. Categories of Data Subjects (e.g., employees, clients, contractors, etc.): _____
c. Purpose(s) of Data Collection: _____
d. Legal Basis for Data Processing (e.g., consent, contractual necessity, legal obligation): _____

Data Handling and Processing

a. Will the data be shared with third parties? (Yes/No/N/A)
   If yes, please specify the third parties: _____
b. Will there be any cross-border transfer of personal data (e.g., transfer outside the Philippines)? (Yes/No/N/A)
   If yes, please specify the recipient country/countries and measures in place to ensure data protection: _____
c. How will the data be stored? (e.g., physical storage, local electronic storage, cloud services): _____
d. Who will have access to the data? (Specify roles, not names):
   _____
e. What is the data retention period? (How long will the data be stored?):
   _____
f. How will the data be securely disposed of when no longer needed? (e.g., data deletion procedures, physical shredding): _____

Privacy Risk Identification

a. Does the project involve sensitive personal data or pose significant risks to data subjects' privacy rights? (Yes/No/N/A)
b. Potential privacy risks identified (e.g., unauthorized access, data breach, accidental loss, misuse): _____
c. Measures in place to mitigate these risks (e.g., encryption, access controls, monitoring, regular audits): _____

Data Protection Measures

a. Are physical security measures in place (e.g., ID badges, restricted access areas, CCTV, physical locks)? (Yes/No/N/A)
b. Are technical security measures in place (e.g., encryption, secure passwords, firewalls, intrusion detection systems)? (Yes/No/N/A)
c. Are organizational measures implemented (e.g., staff training, data protection policies, incident management plans)? (Yes/No/N/A)
d. Are measures regularly reviewed, updated, and tested to ensure continuous data protection? (Yes/No/N/A)

If Yes to any of the above, please describe the specific measures across physical, technical, and organizational areas: _____

Conclusion and Recommendations

a. Summary of Privacy Risks and Existing Mitigation Measures: _____
b. Recommendations for Strengthening Privacy Protection (if any): _____
c. Does the project/process comply with DPWH's data protection policies and the Data Privacy Act of 2012? (Yes/No/N/A) _____

Certification and Endorsement

Prepared By:
Name: _____
Position: _____
Signature: _____
Date: _____

Reviewed and Endorsed By (Data Protection Officer / Compliance Officer for Privacy):
Name: _____
Position: _____
Signature: _____
Date: _____

Annex F

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

PERSONAL DATA REQUEST FOR ACTION FORM

Data Subject Information

Full Name	
Contact Number	
Email Address	
Address	

Type of Request

☐ Access to my personal data
☐ Correction of my personal data
☐ Erasure or blocking of my personal data
☐ Complaint regarding processing of my personal data
☐ Withdrawal of consent
☐ Other: _____

Description of Request/Concern

Please describe in detail the nature of your request or complaint, including relevant dates, document numbers, or any supporting information.
[Write here]

Supporting Documents Attached

☐ Valid ID with photo and signature
☐ Authorization letter (if filed by a representative)
☐ Other: _____

Declaration and Signature

I declare that the information I have provided is true and correct. I understand that the Department may need to verify my identity and may contact me for further details regarding this request.
Signature: _____
Date: _____

For Official Use Only (To be filled out by the Head of Office)

Date Received	
Received By	
Assigned To	
Action Taken	
Date Completed	
Remarks	

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

PERSONAL DATA SECURITY BREACH REPORT FORM

Incident Details

- **Date and time of breach**: _____
- **Date and time breach was discovered**: _____
- **Reported By**: _____
- **Contact information of reporter**: _____
- **Type of breach** (e.g., unauthorized access, data loss, theft, etc.): _____
- **Method of breach** (e.g., hacking, physical loss, accidental exposure, etc.): _____

Affected Data

- **Categories of personal data affected** (e.g., name, address, email, financial details, health data, etc.): _____
- **Number of individuals affected**: _____
- **Is sensitive personal data involved?** (e.g., race, religion, health, etc.):
  - Yes [ ] No [ ]
- **Description of data affected** (include specific data types, formats, or systems involved):

_____

_____

Breach Impact Assessment

- **Has the breach been contained?** (Yes/No): _____
- **Actions taken to contain the breach** (e.g., password reset, system shutdown, file encryption, etc.):

_____

_____

- **Potential impact on affected individuals** (e.g., financial loss, reputational damage, identity theft, etc.):

_____

_____

Root Cause Analysis

- **How did the breach occur?**

- **Was the breach caused by a technical, human, or organizational failure?**

- **Is further investigation required?** (Yes/No): _____
- **Other contributing factors** (if any):

Notification and Reporting

- **Was the breach reported to relevant authorities (e.g., data protection regulator)?**
  - Yes [ ] No [ ]
- **Date and time of reporting**: _____
- **Method of notification** (e.g., email, phone call, formal report, etc.):

- **Affected individuals notified?**
  - Yes [ ] No [ ]
- **Date and method of notification to individuals**:

Preventive Actions and Follow-up

- **Immediate actions taken to prevent further breaches** (e.g., system updates, employee training, etc.):

- **Plans for long-term prevention and mitigation** (e.g., policy changes, security audits, software enhancements, etc.):

- **Follow-Up Actions or Monitoring Plans**:

- **Follow-Up Actions or Monitoring Plans**:

Additional Notes

- (Provide any additional relevant information related to the breach, its handling, or recovery process):

Prepared by:

(Name of Respective COP)

Noted by:

Undersecretary MARICHU A. PALAFOX
Data Protection Officer
Department of Public Works and Highways

Annex H

Republic of the Philippines
DEPARTMENT OF PUBLIC WORKS AND HIGHWAYS
CENTRAL OFFICE
Manila

DATA BREACH MANAGEMENT LOG

Date and Time of Breach	Reported By	Description of Breach	Type of Data Affected	Immediate Actions Taken	Persons/Offices Notified	Resolution/Remediation Steps	Remarks/Follow-up Actions
Example: April 25, 2025 - 10:30 AM	IT Support Officer	Unauthorized access to the employee records database.	Employee Names, Contact Information, Employment Records	Isolated the affected server, changed all system passwords, and activated the data breach team.	Data Protection Officer, HRMD Head, IT Division Chief	Restored system from backup, enhanced firewall settings and conducted security awareness training.	Monitoring is ongoing; a review of access control policies is scheduled.