



# **DATA PRIVACY MANUAL**

# Table of Contents

---

Title Page	i
Table of Contents	ii
Foreword	iii
Messages	iv
<b>Chapter 1: Background</b>	<b>1</b>
<b>Chapter 2: Introduction</b>	<b>1</b>
<b>Chapter 3: Scope and Limitation</b>	<b>1</b>
<b>Chapter 4: Definition of Terms</b>	<b>2</b>
<b>Chapter 5: Processing of Personal Data</b>	<b>4</b>
<b>Chapter 6: Security Measures</b>	<b>8</b>
<b>Chapter 7: Breach and Security Incident Management</b>	<b>14</b>
<b>Chapter 8: Inquiries and Complaints</b>	<b>16</b>
<b>Chapter 9: Effectivity and Approval</b>	<b>17</b>
Annexes	18

## Foreword

---



In a time when we are the most connected amid the unprecedented digitalization of our global village, safeguarding the privacy and security of personal data has become of paramount importance.

The DILG recognizes the state policy enshrined in *Section 2 of Republic Act No. 10173 or the Data Privacy Act of 2012* that the State protects the fundamental human right of privacy, of communication while ensuring the free flow of information to promote innovation and growth. Hence, I am pleased to present this DILG Data Privacy Manual, a comprehensive guide meticulously crafted to protect the personal information entrusted to the Department by the citizens we serve and even our very own personnel.

Respecting individual privacy is not just a legal obligation but a fundamental human right. This manual serves as a compass, guiding our different operating units in navigating the complex landscape of data processing while upholding the principles of transparency, legitimate purpose, and proportionality. Within this Manual, we will find not just a set of guidelines but a roadmap to a more conscientious and responsible use of personal information. It also addresses timely concepts such as consent, data breach management, and the rights of data subjects.

I, therefore, urge every DILG official and employee using this Manual to internalize its principles and contribute to the cultivation of a privacy-sensitive use of information disclosed to the Department. I extend my appreciation to DILG Assistant Secretary for Plans and Programs Francisco R. Cruz, the Data Protection Officer (DPO) of this Department, and our Information Systems and Technology Management Service (ISTMS), for their dedication in leading the production of this Manual. Your efforts underscore our collective commitment to safeguarding the privacy and rights of individuals. This Manual, which you tirelessly and constantly update to adapt to the needs of our ever-changing society, serves as a constant reminder that our right to our personal information and privacy is inviolable and inherent.

Together, let us build a future, a Bagong Pilipinas, where innovation and progress coexist harmoniously with the protection of personal information.

  
**JUANITO VICTOR C. REMULLA**  
Secretary



## Message

---



This Data Privacy Manual is a manifestation of the Department's strong resolve to ensure compliance with various data protection laws and meet all necessary regulatory requirements of the National Privacy Commission (NPC).

The operations of the Department are highly bound up with data and information that are critical in facilitating both our administrative and technical works. With the issuance of this Manual, we affirm to our employees and clients that we seriously do our job to preserve and protect their fundamental right to privacy and security.

But more importantly, this Manual contributes to the overall efficiency and effectiveness of the Department. As we build a culture of trust and confidence and create a secure environment where we perpetuate and continuously uphold the integrity, availability, and confidentiality of the data and information entrusted to our Department, we nurture a productive organization. And as we transform our operations owing to the ascending trend of breakthrough technologies and the demands of the times, we continue to fortify and strengthen our guards even more against potential privacy and cybersecurity risks.

While we strive to have more robust systems and processes and smooth day-to-day operations within the Department, we hope that our DILG officials and employees will learn by heart and put into practice this Data Privacy Manual. Together with our Data Protection Officer (DPO), let us help make this Department a model agency where data privacy and security of our employees and clients are of paramount importance.

A handwritten signature in blue ink, appearing to read 'LAV', with a long horizontal flourish extending to the right.

**ATTY. LORD A. VILLANUEVA**  
Undersecretary for Operations

## Message

---



As this Department's Data Protection Officer (DPO), it is with utmost humility that I present to you the DILG's first-ever Data Privacy Manual, which encapsulates our collective policies and strategies in support of and adherence to *Republic Act No. 10173 or the Data Privacy Act (DPA) of 2012*, its Implementing Rules and Regulations (IRR), and other subsequent issuances of the National Privacy Commission (NPC).

We extend our warmest gratitude to the Information Systems and Technology Management Service (ISTMS) under the guidance of Director Loida S. Linson and all DILG offices and operating units who participated in the workshops and consultations made and provided significant inputs that have been of great use in this Manual.

In our pursuit of becoming a highly trusted Department and Partner, it is indispensable that we also have a blueprint for our internal policies and strategies on data protection, which primes our organization to better prepare and manage risks associated with personal data processing and eventually deal with emerging data privacy and security challenges.

It may not be known to many, but there is actually a correlation between data privacy and planning in general. For instance, privacy considerations are integrated during program design wherein we also need to find the right mix and strike a balance of innovation with privacy in such a way that we bring off a level of flexibility to our programs and projects that does not imperil our data protection obligations. This is even more evident in monitoring and evaluation wherein privacy also influences program and project outcomes through data minimization and other similar restrictions on the scope of analysis or metrics employed for impact assessment.

Having this Manual fulfills our commitment to our stakeholders, including the personnel within the Department, to respect and diligently protect their personal data and information while we aggressively infuse innovative solutions toward smart and sustainable information system and database interoperability, knowledge management, and information exchange which are incontestably critical components in planning and program implementation.

A handwritten signature in blue ink, appearing to read 'FRANCISCO R. CRUZ', written over a horizontal line.

**FRANCISCO R. CRUZ, CESO III, MMG**  
Assistant Secretary for Plans and Programs and  
DILG-OSEC Data Protection Officer

## Chapter 1: Background

---

*Republic Act No. 10173*, otherwise known as the “*Data Privacy Act (DPA) of 2012*”, seeks to protect the fundamental human right to privacy and security of personal data in various information and communications systems managed by many public and private institutions, including the government. While the main intention is to uphold data privacy and security, the DPA also ensures that growth and development remain unimpeded, considering the crucial role of these information and communications systems in the overall social and economic transformation of the country.

To facilitate compliance with the *DPA*, its *Implementing Rules and Regulations (IRR)*, and other subsequent issuances by the *National Privacy Commission (NPC)*, each Personal Information Controller (PIC) is expected to create its own Data Privacy Manual which will serve as a blueprint that will govern the processing of personal data and implementation of necessary security measures within the jurisdiction of the concerned agency.

## Chapter 2: Introduction

---

The Department of the Interior and Local Government (DILG)-Office of the Secretary (OSEC) recognizes the need to fortify its DPA measures, part of which is creating its Data Privacy Manual. As the Department strives to infuse innovative and productive solutions toward more effective and efficient systems and processes, data protection remains to be a formidable challenge in the exercise of the agency’s mandated powers and functions.

Paramount in facilitating compliance with the DPA, its IRR, and other NPC issuances, the DILG-OSEC Data Privacy Manual does not merely outline the protocols and safeguards for processing personal data throughout its entire lifecycle, but also underscores the importance of adhering to data protection guidelines. Emphasizing its pivotal role in upholding the rights of data subjects and promoting a culture of privacy awareness, this Manual is indispensable in ensuring that all programs, projects, and activities undertaken by offices and operating units within the DILG-OSEC are compliant and aligned with the DPA requirements and obligations.

## Chapter 3: Scope and Limitation

---

This Data Privacy Manual covers the Executive Offices, Bureaus, Services, Regional Offices, and Project Management Offices under the DILG-OSEC. As such, all concerned personnel, regardless of the type of employment or contractual arrangement, are hereby directed to comply with the terms and protocols set out in this Manual.

Further, this governs all information and communications systems that process personal data through manual and/or electronic means. The rights of the data subjects involved therein, which are largely composed of DILG-OSEC officials and employees as well as the Department's clientele, are well-considered in this Manual.

Under the guidance of the designated Data Protection Officer (DPO), regular reviews and updates of this Manual shall be conducted by the DILG-OSEC DPA Technical Working Group and the Secretariat to account for arising issues and/or emerging trends that may have significant implications to data privacy and security.

## **Chapter 4: Definition of Terms**

---

Unless the context otherwise provides, the terms defined in this Manual shall be applied:

1. Commission refers to the NPC created by virtue of the DPA;
2. Compliance Officer for Privacy (COP) refers to the Bureau, Service, and Regional Directors and Heads of Project Management Offices under the DILG-OSEC who shall assist the DPO in ensuring the compliance of their respective offices and operating units with the DPA, its IRR, and other NPC issuances;
3. Consent of the Data Subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the processing of personal data;
4. Data Breach refers to a security incident that leads to unlawful and/or unauthorized processing of personal data under the control of an agency that compromises its availability, integrity, or confidentiality;
5. DPA Secretariat refers to the office or operating unit under the DILG-OSEC designated to provide technical and administrative assistance to the DPO and COPs in various DPA-related matters;
6. Data Protection Officer (DPO) refers to the DILG official of at least the rank of an Assistant Secretary designated by the Secretary of the Interior and Local Government (SILG) to ensure the Department's compliance with the DPA, its IRR, and other NPC issuances;
7. Data Processing System refers to the structure and procedure by which personal data are processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
8. Data Sharing refers to the sharing, disclosure, or transfer to a third party of personal data under the custody of an agency to one or more other agencies;
9. Data Sharing Agreement (DSA) refers to a contract or any similar document that contains the terms and conditions of a data sharing arrangement between and among parties involved;
10. Data Subject refers to an individual whose personal data are being processed;

11. Department refers to the DILG-OSEC composed of its Executive Offices, Bureaus, Services, Regional Offices, and Project Management Offices;
12. Filing System refers to any set of unprocessed information but remains structured in such a way that specific information relating to a particular individual is readily accessible;
13. Information and Communications System refers to a system for processing electronic data, messages, or documents that involves a computer system or other similar device which data are recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, messages, or documents;
14. Process Owner refers to a DILG-OSEC employee tasked with overseeing and managing the data processing, ensuring compliance with relevant data protection guidelines, and implementing measures to safeguard the privacy and security of data subjects;
15. Personal Information refers to any information whether recorded in a material form or not, from which an individual's identity 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;
16. Personal Information Controller (PIC) refers to the DILG-OSEC who controls the processing of personal data for specified and legitimate purposes;
17. Personal Information Processor (PIP) refers to the Executive Offices, Bureaus, Services, Regional Offices, and Project Management Offices under the DILG-OSEC which were authorized to process personal data on behalf of the PIC;
18. Privacy Impact Assessment (PIA) refers to the process undertaken to evaluate and manage the potential impacts on privacy of a data processing system under the DILG-OSEC;
19. Privacy Notice refers to the agency's policy that informs the data subjects of their data privacy rights, what personal data shall be collected from them, and how the agency intends to use such personal data;
20. Privileged Information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication;
21. Processing refers to any operation related to the collection, utilization, and disposal of personal data;
22. Security Breach refers to a situation that has impact or potential to impact on the security of personal data which jeopardizes its confidentiality, integrity, and availability; and,
23. Sensitive Personal Information refers to personal information about (i) an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations; (ii) 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; (iii) issuance 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 (iv) specifically established by an Executive Order or an act of Congress to be kept classified.



## Chapter 5: Processing of Personal Data

---

The Department processes personal data pursuant to the following functions by virtue of *Executive Order No. 262, s. 1987* or “*Reorganizing the Department of Local Government*”, *Executive Order No. 292, s. 1987* or “*The Administrative Code of 1987*”, and *Republic Act No. 6975* or “*The DILG Act of 1990*”:

1. Assist the President in the exercise of general supervision over local governments;
2. Advise the President in the promulgation of policies, rules, regulations, and other issuances on the general supervision over local governments and on public order and safety;
3. Establish and prescribe rules, regulations, and other issuances implementing laws on public order and safety, the general supervision over local governments, and the promotion of local autonomy and community empowerment, and monitor compliance thereof;
4. Provide assistance toward legislation regarding local governments, law enforcement, and public order and safety;
5. Establish and prescribe policies, plans, programs, and projects to promote peace and order, ensure public safety, and further strengthen the administrative, technical, and fiscal capabilities of local government offices and personnel;
6. Formulate plans, policies, and programs that will meet local emergencies arising from natural and human-induced disasters; and,
7. Establish a system of coordination and cooperation among the citizenry, local executives, and the Department to ensure effective and efficient delivery of basic services to the public.

The processing of personal data shall be allowed, provided that concerned offices and operating units under the DILG-OSEC (i) comply with the requirements of the DPA, its IRR, and subsequent issuances from the NPC and (ii) adhere to the principles of transparency, legitimate purpose, and proportionality, as stated in *Section 18, Rule VI (Data Privacy Principles) of the DPA’s IRR*:

1. Transparency, wherein the data subjects must be aware of the nature, purpose, and extent of the processing of their personal data, including the risks and safeguards involved and their privacy rights as data subjects;
2. Legitimate Purpose, wherein the processing of personal data should have a declared and specified purpose compliant with existing and applicable laws, rules, and regulations; and,
3. Proportionality, wherein the processing of personal data should be adequate, relevant, suitable, necessary, and not excessive in relation to the declared and specified purpose.

### Collection

Pursuant to *Section 19 (a), Rule VI (Data Privacy Principles) of the DPA’s IRR*, the following must be primarily considered in the collection of personal data:

1. It must only be undertaken for a specified, declared, and legitimate purpose;
2. There should be consent prior to the collection, which the PIC or the concerned PIP should properly document as proof and reference;
3. The purpose must be declared before collection unless not reasonable nor practicable, in which case it should be declared after collection but before any further processing; and,
4. The personal data to be collected should not be excessive and must be reconcilable with the declared, specified, and legitimate purpose.

The guidelines in developing consent forms as well as obtaining and withdrawing thereof must comply with *NPC Circular No. 2023-04* dated 07 November 2023.

The Department collects personal data through the use of information and communications systems and/or manual accomplishment of forms and documents. The collection should always be accompanied by a Privacy Notice that contains the following information:

1. Personal data collected and the manner of collection;
2. Basis, use, and purpose for processing of personal data;
3. Methods utilized for automated access;
4. Disclosure of personal data;
5. Risks involved and data protection and security measures;
6. Storage, retention, and disposal of personal data;
7. Rights of data subjects; and
8. Complete contact information of the DPO or the concerned COP.

While consent may not be required in certain instances when it is not relied on as basis for processing personal data, a Privacy Notice is required at all times for data subjects to be informed of the processing of their personal data and their rights as data subjects.

The Privacy Notice should be transparent, compelling, and communicated using clear and plain language. It should be displayed alongside the NPC Seal of Registration issued to the Department.

### **Processing**

The actual processing should be done fairly and lawfully to ensure the quality and integrity of personal data. As provided in *Section 19 (b) and 19 (c), Rule VI (Data Privacy Principles) of the DPA's IRR*, the following must be considered:

1. Processing must be in a manner compatible with the declared, specified, and legitimate purpose;

2. Processed personal data should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
3. Processing shall be undertaken in a manner that ensures appropriate privacy and security safeguards;
4. Personal data should be accurate and where necessary for declared, specified, and legitimate purpose, kept up to date; and,
5. Inaccurate or incomplete data must be rectified, supplemented, destroyed, or their further processing restricted.

### **Storage, Retention, and Destruction**

As provided in *Section 19 (d), Rule VI (Data Privacy Principles) of the DPA's IRR*, personal data collected must be kept and stored in safe storage, whether physical or electronic, until the fulfillment of the declared, specified, and legitimate purpose or as provided by the law.

The retention period shall be set on the following grounds:

1. For documents utilized for administrative, budgetary, and legal purposes, the retention period should follow existing and applicable laws, rules, and regulations, i.e. Commission on Audit (COA), Civil Service Commission (CSC), Freedom of Information (FOI), Anti-Red Tape Authority (ARTA) Circulars, among others;
2. For other public records, the retention period should follow *Republic Act No. 9470 or the "National Archives of the Philippines Act of 2007" and its IRR*, and *DILG Circular No. 2016-03 on the Guidelines and Procedures on Disposal of Records and Use of Records Disposition Schedule (RDS)*; and,
3. Other databases should follow the retention period specified in their respective PIAs.

After the attainment of its declared, specified, and legitimate purpose or as provided by the law, the personal data must be disposed of or discarded in a secure manner to prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects, such as but not limited to:

1. Shredding of physical documents;
2. Permanent deletion of online databases; and,
3. Permanent deletion of softcopy databases in backup drives.

### **Access, Disclosure, and Sharing**

Access to any storage or databases containing personal and confidential data, whether physical or electronic, should only be limited to authorized personnel to be determined by the concerned COP.

Any request for accessing the storage and database must be approved by the concerned COP, DPO, or SILG depending on the nature, purpose, and extent of the processing of personal data.

Pertinent provisions of *Republic Act No. 11032 or the "Ease of Doing Business and Efficient Government Service Delivery Act of 2018"* and its IRR shall govern in responding and complying with such requests. Further, requests for personal data of public officials and employees must be compliant with the guidelines set forth in *NPC Circular No. 2022-01* dated 04 February 2022.

The DILG-OSEC only shares personal data if required by law, prescribed by existing and applicable rules and regulations, or if necessary, for compliance associated with a Data Sharing Agreement (DSA) to keep and treat all personal data confidential.

The SILG is authorized to participate in a DSA with other government agencies and private institutions while the DPO acts as a witness thereof. The concerned COP is also authorized to negotiate the DSA with other involved parties, provided that the same be consulted with the DPO and the Legal and Legislative Liaison Service (LLLS) before securing its approval.

Further, the DSA must comply with *NPC Circular No. 2020-03* dated 23 December 2020, particularly its contents which must include the purpose and lawful basis for entering into such an agreement, the objectives, parties, and terms involved, the operational details, security, and rights of data subjects, and the retention and data disposal, as provided in *Section 9 (Contents of a Data Sharing Agreement)*.

### **Rights of the Data Subjects**

The data subjects have full control over their personal data and thus possess the following rights under *NPC Advisory No. 2021-01* dated 29 January 2021:

1. Right to be informed, wherein the data subject has the right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling;
2. Right to object, wherein the data subject shall have the right to object to the processing of his or her personal data where such processing is based on consent or legitimate interest;
3. Right to access, wherein the right of data subjects to access information on the processing of their personal data shall be subject to the following: (i) right to obtain confirmation on whether or not data relating to him or her are being processed and other related information; (ii) right to only request access to his or her own personal data and other related information and not to the information relating to any other individual; and, (iii) limits to the right to access if such requests have already been made public, have been repetitive and entailed disproportionate amount of effort and resources, and have implications to safety and security of the data subject;

4. Right to rectification, wherein the data subject has the right to dispute the inaccuracy or error in his or her personal data and have the PIC correct the same within a reasonable period of time;
5. Right to erasure or blocking, wherein the data subject has the right to request for the suspension, withdrawal, blocking, removal, or destruction of his or her personal data from the PIC's filing system, in both live and back-up systems;
6. Right to data portability, wherein the data subject has the right to obtain from the PIC a copy of his or her personal data and/or have the same transmitted from one PIC to another, in an electronic or structured format that is commonly used and allows further use by the data subject; and,
7. Right to damages, wherein the data subject has the right to be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of their personal data, taking into account any violation of his or her rights and freedoms as data subject.

## Chapter 6: Security Measures

---

The DILG-OSEC as the PIC shall implement appropriate security measures to protect personal data under its custody against natural or accidental loss or destruction and human threats such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination while keeping its availability, integrity, and confidentiality.

### Organizational Security Measures

Where appropriate, all offices and operating units under the DILG-OSEC shall comply with the following guidelines for organizational security:

1. Designation of DPA Officers
  - (i) The DPO shall be at least the rank of an Assistant Secretary and accountable for the PIC's compliance with the DPA, its IRR, and other NPC issuances;
  - (ii) The COPs shall be composed of Bureau, Service, and Regional Directors and Heads of Project Management Offices under the DILG-OSEC to assist the DPO in ensuring the compliance of their respective offices and operating units with the DPA, its IRR, and other NPC issuances;
  - (iii) The DPA principal and alternate focal persons for each Bureau, Service, Regional Office, and Project Management Office shall be at least the level of a Section Chief or its equivalent to assist the COPs in monitoring the compliance of their respective offices and operating units with the DPA, its IRR, and other NPC issuances;

- (iv) The process owners for each data processing system managed by and under the custody of Bureaus, Services, Regional Offices, and Project Management Offices shall ensure that processing undertaken are compliant with the DPA, its IRR, and other NPC issuances;
- (v) The Data Breach Response Team for each Bureau, Service, Regional Office, and Project Management Office shall adhere to its duties and obligations and ensure swift and effective resolution of any reported data breach incidents;
- (vi) The DPA Secretariat shall provide the overall technical and administrative assistance to the DPO and COPs, particularly in implementing and monitoring various data security policies within the jurisdiction of the DILG-OSEC; and,
- (vii) The designation of DPA officers must be formalized through the issuance of a Department or Special Order or an Office Order designating DILG-OSEC officials and employees.

## 2. Registration of the DPO, COPs, and Data Processing Systems

- (i) Registration of the DPO, COPs, and data processing systems shall follow the guidelines outlined in *NPC Circular No. 2022-04* dated 05 December 2022;
- (ii) The PIC shall register its DPO, COPs, and data processing systems through the NPC Registration System (NPCRS) at <https://npcregistration.privacy.gov.ph>;
- (iii) The details of all data processing systems owned by the PIC at the time of initial registration shall be encoded into the platform;
- (iv) All offices and operating units under the DILG-OSEC shall submit to the DPO a brief description of each data processing system as stipulated under *Section 12 (B) of NPC Circular No. 2022-04*;
- (v) The registration or renewal process shall be done by the DPO with the assistance of the DPA Secretariat;
- (vi) The PIC shall register its newly implemented data processing system or inaugural DPO within 20 days from the commencement of such system or the effectivity date of such appointment;
- (vii) In the event that the PIC seeks to apply minor amendments to its existing registration information, which includes updates on an existing data processing system or a change in DPO, the PIC shall update the system within 10 days from the system update or effectivity of the appointment of the new DPO; and,
- (viii) Once the NPC has issued the Department with the Seal of Registration, the DPO with the help of the DPA Secretariat shall facilitate the display of the Seal on the DILG official website, and in the case of COPs, in their respective buildings and offices, preferably at the lobby or entrance halls for employees and visitors.

## 3. Conduct of Privacy Impact Assessment (PIA)

- (i) A PIA shall be conducted to evaluate and manage impacts on the privacy of a particular data processing system;
- (ii) All data processing systems shall undergo PIA and shall become a requirement prior to its implementation;
- (iii) The conduct of the PIA shall follow the guidelines provided in *NPC Advisory No. 2017-03* dated 31 July 2017 and the internal policy on the conduct of the PIA to be issued by the DPO;
- (iv) All offices and operating units under the DILG-OSEC shall submit to the DPO the PIA duly endorsed by the concerned COP for review and approval, and if necessary, implement comments and/or recommendations by the DPO or DPA Secretariat as a result of the review undertaken;
- (v) The DPA Secretariat shall serve as the repository of all approved PIAs; and,
- (vi) The PIA shall be conducted at least every three (3) years or whenever necessary following updates or new features to be implemented in the data processing system.

#### 4. Conduct of Training, Seminars, and Workshops

- (i) Regular training, seminars, and workshops of at least once every semester must be provided for the DPO, COPs, DPA focal persons, and process owners under the DILG-OSEC to keep them updated on the developments and new policies related to data privacy and security;
- (ii) Aside from DPA officers, all employees under the DILG-OSEC must also be oriented on various DPA-related policies, including their rights as data subjects, at least once every semester;
- (iii) The DPA Secretariat in consultation with the DPO shall facilitate the provision of these orientations and capacity development interventions; and,
- (iv) For those DPA-related training, seminars, and workshops initiated by other offices and operating units under the DILG-OSEC, the same should be coordinated with the DPO and DPA Secretariat for proper guidance to ensure harmony and coherence in terms of provision of DPA-related capacity development interventions.

#### 5. Records of Processing

- (i) All requests for access to databases, whether physical or electronic, must clearly state the purpose and valid justification for such a request, subject to approval by the concerned COP, DPO, or SILG depending on the nature, purpose, and extent of access to these personal data;
- (ii) All employees with access to sensitive personal and privileged information must duly note and practice the *Duty of Confidentiality* and therefore be compelled to sign a Non-Disclosure Agreement (NDA); and,

- (iii) Concerned offices and operating units must ensure that there is a record of information flow, from the collection process, utilization or attainment of the purpose, and retention of the personal data until disposal or destruction, such as but not limited to consents, NDAs, DSAs, among others.

#### 6. Review of the Data Privacy Manual

- (i) This Manual shall be reviewed and evaluated annually such that existing data privacy and security policies and practices within the DILG-OSEC shall remain consistent and aligned with new or amended laws, rules, and regulations; and,
- (ii) The DPO with the assistance of the DPA Secretariat shall facilitate the review of this Manual, and if necessary, appropriate capacity development interventions and consultations with the NPC must be undertaken to ensure that any modification implemented as a result of the review remains appropriate and consistent with existing and applicable laws, rules, and regulations.

#### 7. Supplementary Policies, Violations, and Sanctions

- (i) As deemed necessary, the DPO can issue Memoranda and Advisories, or the SILG in the case of Circulars, Memorandum Circulars, and Department and Special Orders, as supplementary policies and guidelines relative to the DILG-OSEC's compliance with the DPA, its IRR, and other NPC issuances;
- (ii) Any minor offense or violation of the DPA policies outlined in this Manual and other DPA-related issuances may result in a formal and official written warning through a Memorandum, outlining the nature and extent of the offense or violation committed and providing guidance and recommendations to the concerned office or operating unit or involved personnel on the corrective actions to be undertaken;
- (iii) In extreme cases, where the offense or violation involves significant harm, intentional misconduct, or a breach of legal requirements, the Department may opt for legal action, potentially resulting in fines or other legal consequences, pursuant to the DPA, its IRR, and other NPC issuances, particularly *NPC Circular No. 2022-01* dated 08 August 2022; and,
- (iv) The DPO and DPA Secretariat shall serve as the repository of all DPA policies and related issuances, including documents pertaining to offenses or violations thereof.

#### 8. Monitoring and Reporting

- (i) The DPO with the help of the DPA Secretariat shall lead the monitoring and whenever necessary, may conduct compliance checks in the form of privacy sweeps, document submissions, onsite visits, among other modes;



- (ii) The DPA Secretariat shall also conduct a review of all existing data processing systems under the DILG-OSEC and submit significant findings and recommendations thereof to the DPO; and,
- (iii) Any DPA-related issues and concerns must be directly reported to the DPO or concerned COP through their official contact details.

### **Physical Security Measures**

Where appropriate, all offices and operating units under the DILG-OSEC shall comply with the following guidelines for physical security:

#### **1. Storage Facilities**

- (i) Any personal data gathered by the Department through manual and/or electronic means should be securely stored in a facility or electronic medium well-protected from unauthorized access or data breaches;
- (ii) The physical storage of personal data under the custody of the Department must be kept in folders, envelopes, cabinets, and secured rooms;
- (iii) Storage devices such as external hard drives must be kept in a secured facility when not in use, wherein only known devices properly configured to the Department's security standards are authorized to access such personal data; and,
- (iv) Portable storage facilities such as external hard drives must not be transported or accessed outside of the DILG-OSEC property, unless authorized by the DPO or concerned COP, or the SILG for that matter, depending on the nature and extent of personal data involved, wherein procedures as provided in *Section 31 (b) of the DPA's IRR* shall apply in this case.

#### **2. Access and Process Precautions**

- (i) All personnel authorized to enter and access the data rooms or centers must fill out a logbook placed at the entrance, indicating their name, date, time, and purpose of each request for access;
- (ii) For those storage facilities housing significant amounts of personal data, i.e. data rooms or centers, biometrics machines and CCTV surveillance systems must be installed to ensure that only authorized personnel can access such storage facilities;
- (iii) A *Clear Desk Policy* must be implemented and personal computers must be turned off and protected with passwords to maintain the security of personal data stored therein and ensure that no sensitive personal and privileged information will be displayed and readily accessed by any unauthorized personnel; and,
- (iv) Facilities and equipment used in processing or storing personal data must be secured against natural or human-induced disasters and emergencies or unauthorized external access, data breaches, and other cybersecurity threats.

### 3. Disposal and Retention Procedures

- (i) The Department processes and retains all the necessary personal data according to the purpose;
- (ii) All excessive copies of the documents must be disposed of or destroyed in such a way that these can no longer be obtained again; and,
- (iii) Retention procedures for personal data within the Department's jurisdiction, as provided in this Manual, must be implemented.

### **Technical Security Measures**

The Department through the Information Systems and Technology Management Service (ISTMS) shall implement technical security measures to ensure that there are appropriate and sufficient safeguards to secure the processing of personal data, particularly the network infrastructure and data centers in place, including the required encryption and authentication processes that control and limit access to these facilities.

Personal data acquired or gathered digitally must be stored in a data center and administered by authorized personnel under an NDA. Precautionary measures should be applied in protecting the Department's data center against accidental or unlawful access and alteration of personal data under the possession of the Department. As such, biometrics machine and CCTV surveillance system must be installed to ensure that only authorized personnel can access the data center.

The following protocols must be regularly performed:

1. Security breaches monitoring to ensure that the computer network is protected against accidental, unlawful, or unauthorized access;
2. Conduct of regular testing, assessment, and evaluation of the effectiveness of security measures such as but not limited to the following:
  - (i) Formulate cyber security policies and conduct regular reviews of their applicability;
  - (ii) Conduct vulnerability assessments and perform penetration testing within the Department on a regular schedule to be determined by the appropriate office or operating unit; and,
  - (iii) Review, evaluate, and test prior to deployment the software and application systems to ensure the compatibility of security features and overall performance of the device;
3. Installment and implementation of encryption, authentication process, and other technical security measures that control and access personal data:
  - (i) All personal data that are digitally processed must be encrypted, preferably with the Advanced Encryption Standard with a key size of 256 bits (AES-256), with passwords

- or passphrases used to access personal data of sufficient strength to deter password attacks;
- (ii) All authorized personnel who have access to personal data online shall authenticate their identity via a secured connection and mechanisms, i.e. multi-factor authentication, email and mobile verifications, among others;
  - (iii) Access records and procedures shall be reviewed by the DPA secretariat regularly.
4. Implementation of the *DILG ICT Security Policy* which aims to protect the network infrastructure and information systems against accidental, unlawful, or unauthorized access while maintaining the integrity, confidentiality, and availability of the information within the Department in adherence with the DPA, its IRR, and other NPC issuances; and,
  5. Incorporating in the DILG Information Systems Strategic Plan (ISSP) the enhancements in various security measures for DILG digital infrastructures.

## **Chapter 7: Data Breach and Security Incident Management**

---

Following the increasing incidence of personal data breaches that impact both public and private entities, entailing significant economic and legal costs for those involved in processing of personal data and putting at risk data subjects for identity theft, crimes, and other harms, there is a need to establish a policy under this Manual on data breach and security incident management. In particular, *Section 38, Rule IX (Data Breach Notification) of the DPA's IRR and NPC Circular No. 2016-03* dated 15 December 2016 serve as the primary bases for the measures to be implemented under these circumstances:

### **Types of Data Breaches**

1. Availability breach occurs when there is an incident resulting from loss, accidental, or unlawful destruction of personal data;
2. Integrity breach occurs when there is an incident resulting from the alteration of personal data; and,
3. Confidentiality breach occurs when there is an incident resulting from the unauthorized disclosure of or access to personal data.

### **Security Incident Management Policy**

1. Data Breach Response Team

The DILG Data Breach Response Team is an organized group with clearly defined roles and duties, mandated with the responsibility of assessing and evaluating data breach occurrences. They are the designated individuals responsible for reacting to and carrying

out an inquiry in the event of a reported data breach. Each office and operating unit must have its own Data Breach Response Team, all of which fall under the oversight of the DPO.

## 2. Recovery and Restoration of Personal Information

All offices and operating units under the DILG-OSEC must have a backup copy of all the personal data under their custody, subject to applicable guidelines under this Manual. In times of data breach, the backup copy will serve as the basis for determining whether there are inconsistencies or alterations that affect the integrity of the personal data. Moreover, this will also help retrieve or determine the authenticity of lost data.

## 3. Data Breach Notification and Documentation

### (i) Notification

In the event of a data breach, the concerned office or operating must immediately inform the DPO of the incident. The Department through the DPO must then submit a notification report to the NPC through the Data Breach Notification Management System (DBNMS) online platform within 72 hours, which can be accessed via <https://dbnms.privacy.gov.ph>. Additionally, a comprehensive incident report must be provided within five (5) days from the day of the incident identification, unless the Department requests and receives the NPC approval for an extension.

Further, the DPO with the assistance of the DPA Secretariat shall submit an Annual Security Incident Reports (ASIR) to the NPC through the DBNMS.

### (ii) Documentation

All data breach incidents must be thoroughly documented and submitted to the DPO. The report generated during the incident should encompass all pertinent information regarding the nature of the data breach, complete chronology of events, its impact, and the immediate response actions undertaken by the concerned office or operating unit.

## **Data Breach Incident Procedure**

### 1. Assessment of the Incident

- (i) Designate the Officer who will take over the investigation of the breach and take immediate action to stop the breach;
- (ii) Identify the scope and all personal data involved in the incident; and,
- (iii) Document all the initial information and immediate actions taken.

## 2. Breach Impact Reduction

- (i) Identify and separate the compromised personal data;
- (ii) Restore the affected system;
- (iii) Change the encryption key or password; and,
- (iv) Implement a backup process for retrieving and authenticating data.

## 3. Breach Notification

- (i) Submit a full report of the data breach to the DPO within 24 hours upon knowledge or occurrence of the incident;
- (ii) Send notifications to data subjects affected by the data breach incident within 72 hours upon knowledge of the possible or actual data breach incident; and,
- (iii) Send notification to the NPC within 72 hours upon knowledge of the possible or actual data breach incident.

## 4. Post-Data Breach Incident

- (i) Provide inquiry assistance to the data subject affected by the data breach incident;
- (ii) Continue the monitoring and evaluation of the system;
- (iii) Investigate the gap in the system and evaluate the data management policy;
- (iv) Update system security and data management policy;
- (v) Regularly conduct the PIA of the system affected; and,
- (vi) Provide a report of the monitoring and evaluation to the DPO.

# Chapter 8: Inquiries and Complaints

---

For inquiries and complaints, the data subjects may contact the DPO or the concerned COP:

**FRANCISCO R. CRUZ, CESO III, MMG**

Assistant Secretary for Plans and Programs

DILG-OSEC Data Protection Officer

dilg.dpo2024@gmail.com

Landline No.: 8876-3454 local 3303

## Chapter 9: Effectivity and Approval

---

All internal policies inconsistent herewith in part or in full, are hereby modified, revoked, or repealed accordingly. This Manual shall take effect immediately.


Prepared by:



---

**FRANCISCO R. CRUZ, CESO III, MMG**  
Assistant Secretary for Plans and Programs  
DILG-OSEC Data Protection Officer

Approved by:



---

**JUANITO VICTOR C. REMULLA**  
Secretary of the Interior and Local Government

**DEC 10 2024**

---

Date

## Annexes

---

*Republic Act No. 10173 or the “Data Privacy Act of 2012”*

Link: <https://privacy.gov.ph/data-privacy-act>

*Implementing Rules and Regulations of Republic Act No. 10173 or the “Data Privacy Act of 2012”*

Link: <https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012>

National Privacy Commission Circulars and Advisories

Link: <https://privacy.gov.ph/pips-and-pics/advisories-circulars>