



Republic of the Philippines
DEPARTMENT OF ENERGY

DEPARTMENT ORDER NO. DO2022-05-0007 *ff*

**GUIDELINES ON THE IMPLEMENTATION OF DEPARTMENT OF ENERGY
DATA PRIVACY AND INFORMATION SECURITY SYSTEMS AND SOLUTIONS AND
CREATION OF THE DATA PRIVACY COMMITTEE, DATA BREACH RESPONSE
TEAM AND DATA PROTECTION TEAM**

WHEREAS, Republic Act (R.A.) No. 10173, otherwise known as the “Data Privacy Act (DPA) of 2012”, recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

WHEREAS, in compliance with R.A. No. 10173 and its Implementing Rules and Regulations (IRR), a Data Privacy Committee (DPC) is hereby established to facilitate the formulation and implementation of the Data Privacy Program of the Department;

WHEREAS, pursuant to National Privacy Commission Circular 16-03 (“Personal Data Breach Management”) a Data Breach Response Team (DBRT) and Data Protection Team (DPT) are likewise established to execute the herein Guidelines on Data Privacy and Information Security Systems and Solutions that provide administrative protocols and standards set forth in the Data Privacy Manual to ensure that personal information collected are processed in accordance with the general principles of transparency, legitimate purpose and proportionality;

NOW, THEREFORE, in view of the foregoing premises, the following Guidelines are hereby issued:

SECTION I. POLICY STATEMENT

1. DOE is committed to keeping the personal information of its clients, employees, applicants, and vendors accurate, confidential, and secure.
2. DOE has designed this implementing Guidelines to ensure compliance with relevant internal and external policies, rules, and procedures.

3. DOE shall adhere to the general guidelines as embodied in the Implementing Rules and Regulations of the DPA (DPA IRR), which are similarly described as follows:
 - a. Protection of every individual's right to privacy while ensuring free flow of information in order to promote innovation, growth, and national development;
 - b. Recognition of the vital role of information and communications technology (ICT) in nation-building and enforcement of the State's inherent obligation to ensure that personal data in information and communications systems in the government and in the private sector are secured and protected;
 - c. Regulation in the processing of personal information and, in certain cases, processing of sensitive personal information and privileged information;
 - d. Protection of personal information through the implementation of reasonable and appropriate organizational, physical, and technical security measures.

Any offense or violation of this Guidelines shall be dealt with according to Philippine laws and/or relevant Civil Service rules and regulations.

SECTION II. OBJECTIVES

This Guidelines aims to:

1. Provide guidance in complying with the requirements under the DPA and other relevant rules and regulations;
2. Ensure that all personal information of natural and juridical persons in the government or private sector are collected, used, transferred, stored, and disposed in accordance with the rules mandated in the DPA;
3. Recognize the accountabilities of DOE in safeguarding all personal information controlled and processed; and,
4. Establish processes for addressing breaches and violations based on legal, ethical, and proper boundaries.

SECTION III. SCOPE AND APPLICATION

1. This Guidelines applies to all DOE officials and employees using, in part or in full, any of the DOE ICT resources including, but not limited to, computers and their peripherals, auxiliary devices, Local Area Network (LAN), mobile devices (e.g., mobile data/pocket WIFI, and tablets), software, and other ICT facilities;

2. This shall also apply to all DOE officials and employees, regardless of the type of employment or contractual arrangement, and to the extent practicable, agents, suppliers, clients, concessionaires, guests, lessors, tenants, consignors, customers, and other persons who may receive personal information from DOE, have access to personal data collected or processed by or on behalf of DOE, or who provide information to the agency; and
3. All non-DOE personnel or individuals who are allowed or authorized to use any of the DOE ICT resources are likewise covered by this Guidelines. The authorizing DOE personnel shall be accountable and responsible for ensuring compliance with the stipulations laid down in this Guidelines.

SECTION IV. DEFINITION OF TERMS

The Definition of Terms found in **Annex A** shall be used and shall form an integral part of this Guidelines.

SECTION V. CREATION OF THE DATA PRIVACY COMMITTEE, DATA BREACH RESPONSE TEAM AND DATA PROTECTION TEAM

1. *Composition.*

DATA PRIVACY COMMITTEE

Data Protection Officer (DPO)	-	Director, ITMS
Compliance Officer for Privacy (COP)	-	Director, Legal Services
Personal Information Controller (PIC)	-	All Bureau Directors All Services Directors Field Offices Directors
Personal Information Processors (PIP)	-	All Division Chiefs

DATA BREACH RESPONSE TEAM

Personal Information Processors
Data Protection Team

DATA PROTECTION TEAM

Office of the Director, ITMS
Information Technology Division
Information Data Management Division

2. **Functions.**

DATA PRIVACY COMMITTEE

Data Protection Officer

- a. Monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the National Privacy Commission (NPC) and other applicable laws and policies. For this purpose, the designated DPO may:
 1. Collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
 2. Analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
 3. Inform, advise, and issue recommendations to the PIC or PIP;
 4. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and,
 5. Advise the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law.
- b. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- c. Advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);
- d. Ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation, and submission to the NPC of reports and other documentation concerning security incidents or data breaches within the prescribed period;
- e. Inform and cultivate awareness on privacy and data protection within the organization, including all relevant laws, rules and regulations and issuances of the NPC;

- f. Advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design approach;
- g. Serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC and other authorities in all matters concerning data privacy or security issues or concerns;
- h. Cooperate, coordinate, and seek advice of the NPC regarding matters concerning data privacy and security; and,
- i. Perform other duties and tasks that may be assigned by higher authority that will further the interest of data privacy and security and uphold the rights of the data subjects.

Compliance Officer for Privacy

Except for items (a) to (c), the COP shall perform all other functions of the DPO. Where appropriate, COP shall also assist the supervising DPO in the performance of his functions.

The DPO and COP must have due regard for the risks associated with the processing operations of the PIC or PIP, taking into account the nature, scope, context and purposes of processing. Accordingly, they must prioritize their activities and focus their efforts on issues that present higher data protection risks.

Personal Information Controllers / Personal Information Processors

- a. Effectively communicate to its personnel, the designation of the DPO and COP and their functions;
- b. Allow the DPO and COP to be involved from the earliest stage in all issues relating to privacy and data protection;
- c. Provide sufficient time and resources necessary for the DPO and COP to keep themselves updated with the developments in data privacy and security and to carry out their tasks effectively and efficiently;
- d. Grant the DPO and COP appropriate access to the personal data it is processing, including the processing systems;

- e. Where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;
- f. Promptly consult the DPO and COP in the event of a personal data breach or security incident; and,
- g. Ensure that the DPO and COP are involved in all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.

DATA BREACH RESPONSE TEAM

- a. Implement procedures in accordance with the Personal Data Breach Management Manual for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
- b. Facilitate clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure who shall be immediately contacted in the event of a possible or confirmed personal data breach;
- c. Conduct of a preliminary assessment to:
 - i. Assess, as far as practicable, the nature and scope of the personal data breach and the immediate damage;
 - ii. Determine the need for notification of law enforcement or external expertise; and,
 - iii. Implement immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system.
- d. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach and its potential harm and negative consequences to affected data subjects;
- e. Implement procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;
- f. Conduct of investigations that will evaluate fully the security incident or personal data breach which involves possible commission of criminal acts;
- g. Implement procedures for notifying the NPC and data subjects when the breach is subject to notification requirements. The PIC shall promptly notify the Commission and the affected data subjects; and,

- h. Implement policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The DPC must be ready to provide assistance to data subjects whose personal data may have been compromised.

DATA PROTECTION TEAM

The DPT shall to assist the DPO in observance of his/her duties. The DPT may be delegated by the DPO to perform certain duties and responsibilities of the DPO.

SECTION VI. COLLECTION OF PERSONAL INFORMATION

The Department shall collect only those personal information of data subjects which are adequate, necessary, and relevant, and must proceed in a manner compatible with declared, specified, and legitimate purpose.

Collection of personal information must not be excessive and shall be limited only to information necessary in the fulfillment of the Department's mandate and contracted obligations.

Personal information of data subjects shall be collected with the consent of data subjects as to the use, retention, transfer or disclosure, and disposal of personal information, except, if necessary to carry out the functions of public authority, subject to the rules provided by the DPA and other applicable laws and regulations.

1. Manual Transactions

For personal information collected manually or using a paper-based format (*i.e.*, through hard copy forms, letters, reports, and the like), the following guidelines must be followed during the collection process:

- a. Privacy notice must be either indicated in the forms or indicated in a separate file format (annexed to collection forms or through a standee) to notify data subjects regarding the purpose of collecting personal information.
- b. Collection of personal information must not be excessive and shall be limited only to information necessary to conduct the Department's operations.
- c. Paper-based records shall be enclosed in a sealed envelope or box.

Documents containing personal information should always be kept in a folder or envelope and should not be left unattended and publicly visible.

As much as possible, paper-based records should not be transferred through a commercial courier, rather, it should be transported through registered mail or by a designated staff.

2. Website or Online Platform

For collection of personal information through the Department's website, the following guidelines shall be followed:

- a. A notice must be indicated in the online application form to inform clients regarding the purpose and use of their personal information.
- b. Personal information required in the forms should not be excessive and limited only to the necessary information needed in the conduct of the Department's operations.
- c. The website of the Department should be protected against unauthorized access.

3. Electronic Mail, Microsoft Teams, Zoom

All documents with personal information received through the DOE email and other collaborative platforms like Microsoft Teams, Zoom, and the like should be stored in a secured server and should be deleted from email inbox after one (1) month.

All emails should contain a footnote stating that all personal information contained therein are confidential and must not be used or transferred for purposes other than those which are declared in the Privacy Notice. The same statement should be communicated to participants prior to collecting personal information when using such collaborative platforms.

All individuals who have access to functional DOE email must be authorized to collect personal information.

4. Network transfer or shared folder, USB flash drive, CD/DVD

Personal information stored in shared folder or that might be collected thru USB flash drive or CD/DVD should only be accessible by concerned units.

There shall be a required authentication of encrypted data, such as unique account names and passwords, prior to the access of personal information from the shared folder, USB flash drive, or CD/DVD.

Files being transferred through the shared folders, USB flash drive, or CD/DVD should be encrypted or protected with passwords.

SECTION VII. STATEMENT OF PURPOSE, RETENTION, TRANSFER OR DISCLOSURE, DISPOSAL, AND UNNECESSARY RECEIPT OR SHARING BY MISTAKE OF PERSONAL INFORMATION

1. Statement of Purpose

- a. Statement of Purpose and Permitted Use should be up-to-date and accessible to all bureaus collecting personal information directly from the data subjects (employees, patients, vendors, and others – e.g. visitors); and,
- b. The Department may only process personal information collected from data subjects in accordance with the following:
 - i. Statement of Purpose and Permitted Use communicated in the physical or electronic forms filled out during the collection process; and,
 - ii. DPA and other applicable laws.

2. Statement of Retention

- a. Statement of Retention should be up-to-date and accessible to all bureaus collecting personal information directly from the data subjects; and,
- b. The Department is to retain data collected from data subjects in accordance with the Statement of Retention, which is patterned and aligned with the Records Disposition Schedule (RDS), communicated in the physical or electronic forms used in the collection process.

3. Statement of Transfer or Disclosure

- a. Statement of Transfer or Disclosure should be up-to-date and accessible to all bureaus collecting personal information directly from the data subjects;
- b. The Department is to transfer personal information internally or to third parties, in accordance with the Statement of Transfer or Disclosure communicated in the physical or electronic forms used in the collection process;
- c. Personal information should not be transferred through email unless the attached documents are encrypted with passwords sent separately in another email and such transfer is vital to the fulfillment of the Department's mandate and operations.

4. Statement of Disposal

- a. Statement of Disposal should be up-to-date and accessible to all departments collecting personal information directly from the data subjects namely, employees, patients, vendors, and others; and,
- b. The Department is to dispose personal information in accordance with the Statement of Disposal, which is patterned and aligned with the Records Disposition Schedule (RDS), communicated in the physical or electronic forms used in the collection process.

5. Unnecessary receipt or sharing by mistake of personal information

Any stakeholder receiving unsolicited personal information should notify sender of personal information of his receipt. Unsolicited personal information should be promptly destroyed or returned to the sender in accordance with the guidelines set forth in Item 2.10 of the DOE Data Privacy Act Manual.

On the other hand, any stakeholder sharing personal information by mistake should be notified immediately and the information shared must immediately be deleted or destroyed by the recipient.

Consequently, for the abovementioned circumstances, the stakeholder should immediately report it to the Data Protection Officer (DPO). He or she must provide the DPO all the necessary details related to the incident. The DPO shall then notify any individual/s affected by the possible privacy breach.

SECTION VIII. USE OF PERSONAL INFORMATION

1. Personal information shall be used only for its declared, specified, and legitimate purpose;
2. Personal information shall only be used to the extent necessary for the fulfillment of the legal mandate of the Department;
3. Access to personal information should be limited only to concerned Bureaus/Services/Offices;
4. Approval of the DPO must first be obtained prior to access and use of personal information of data subjects;
5. In conducting the Department's functions and operations, personal information collected shall be limited to that information necessary to complete the required services; and,

6. For all other purposes, personal information shall be de-identified or aggregated.

SECTION IX. DISCLOSURE OF PERSONAL INFORMATION

1. Limitation on disclosure of personal information;
 - a. Personal information shall only be disclosed in such cases permitted by law or when it is necessary in the performance of the Department's functions and in compliance with laws and regulations; and,
 - b. Approval from the DPO must first be obtained prior to the disclosure of personal information.
2. Disclosure of personal information other than the purpose for which it was collected;
 - a. Personal information shall not be disclosed for any other purpose unless such disclosure is necessary to the fulfillment of the Department's mandate and operations. The same shall be subject to the rules set forth under the DPA and other relevant laws and regulations;
 - b. Disclosure of de-identified information is permitted for purposes of aggregation and analysis;
 - c. Approval of the DPO must be obtained prior to the disclosure of personal information for purposes other than those for which it was collected;
 - d. Confidentiality and Non-Disclosure Agreement shall be executed between the Department and a third-party before the disclosure takes place;
 - e. Disclosure of personal information is permitted for purposes of aggregation and analysis; and,
 - f. Prior to the disclosure of personal information, the DPO shall review the information to assess the risk of inadvertent disclosure of person's identity, taking into account the recipient of the information and the purpose of disclosure.
3. Request by an individual to access his or her personal information;

The Department will provide personal information to an individual or to his or her legal representative regarding the use, disclosure, and existence of his or her personal information when:

- a. Written request is submitted;

- b. Individual or his/her legal representative provides a copy of a valid government-issued proof of identity, such as Philippine passport, driver's license PhilHealth ID, SSS UMID card, Postal ID, TIN ID, Voter's ID, PRC ID or National ID System;
- c. The Department is legally allowed to provide the information; and,
- d. The information is not subject to litigation privilege.

The request shall include:

- a. Full name of the individual that is the subject of the request;
- b. The individual's complete date of birth;
- c. IDs to prove the individual's identity;
- d. If the requestor is the legal representative, the following must be provided:
 - Full name of the requestor
 - Authorization letter
 - Valid government-issued ID as a proof of identity
- e. Date of request;
- f. Requester's current address;
- g. Requester's signature;
- h. A notarized affidavit certifying the individual's identity; and,
- i. The Department may charge for processing the request to cover the expenses incurred for the retrieval, formatting, and delivering of personal information requested.

4. Requirement for Data Sharing Agreement; and,

- a. A Data Sharing Agreement shall be executed between the Department and third parties prior to the sharing or disclosure of personal information of data subjects; and,
- b. Data subject must be informed prior to the collection, use, and disclosure of personal information to the third-party entities that his or her information will be shared.

5. Requirement for third-party service agreement.

- a. A formal Third-Party Service Agreement (TPSA) shall be executed in cases where a service from a third-party is needed in the conduct of the Department's operations. The agreement shall be subject to the minimum content requirements duly specified in the DOE Data Privacy Manual and must adhere to the data privacy principles laid down in the DPA, its IRR, and all issuances of the NPC; and,
- b. Only the authorized person may legally bind the Department to the terms and conditions of the TPSA.

SECTION X. CONDUCTING PRIVACY IMPACT ASSESSMENT

1. The DBRT shall conduct Privacy Impact Assessment (PIA) to any concerned Bureaus/Service/Offices in the following events:
 - a. There is an additional process to be conducted by the bureaus and divisions that have not been assessed in the PIA Tool before;
 - b. There are changes, *i.e.*, document changes, made on the processes conducted by the department significantly affecting scope of processing of personal information;
 - c. Every after implementation of new process, programs, and Data Processing System;
 - d. When introducing new systems for storing and accessing personal information;
 - e. When using existing systems and data for new and unexpected or more intrusive purpose; and,
 - f. When conducting an internal audit of existing systems or activities (both automated and manual).
2. The results of the most recent PIA shall be uploaded to the Department's network folder for Data Privacy documentation; and,
3. PIA can be conducted annually for existing processes, programs, and Data Processing Systems on DPO's discretion and the choice must be documented in the PIA Detailed Plan.

SECTION XI. PRIVACY BREACHES, COMPLAINTS, AND INQUIRIES

1. General Principles in identifying breach of data privacy;
 - a. Personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal information transmitted, stored, or otherwise processed; and,
 - b. A breach may be self-identified through the course of everyday work;
 - c. A breach may be reported via privacy complaint or challenge to compliance filed by a third-party filed within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred by a third-party to the Department addressed to the DPO, who shall refer the same to the DPT for resolution;
 - d. Personal data breach or potential breach may be signaled by the discovery that:

- i. Personal information is found in unexpected context, location, quantity, or format;
 - ii. The Data Privacy Manual is not being adhered to;
 - iii. Terms and conditions regarding handling of personal information are not being adhered to; and,
 - iv. Any individual shall report breach of data privacy to the DPO as soon as possible.
- e. The DBRT, through the guidance of the DPO, shall implement policies, procedures, and guidelines for security incidents and personal data breach. The policies, procedures and guidelines, at a minimum, shall include the following:
 - i. Data Breach Management Program;
 - ii. Cascading of breach reports to the DBRT;
 - iii. Measures to prevent and minimize occurrence of breach and security incidents;
 - iv. Procedures for recovery and restoration of personal data;
 - v. Notification Protocol that within 72 hours, the data breach should be reported to NPC;
 - vi. Documentation and reporting procedure of security incidents or personal data breach; and
 - vii. Conduct of security awareness and data breach drills for officials and personnel.
- f. In accordance with NPC Circular 16-03 Personal Data Breach Management, the DPO shall annually submit a general summary of the reports to NPC; and,
- g. Further reference shall be made through the Guidelines on Personal Data Breach Management.

2. Reporting of Data Privacy Breach

- a. Any individual who discovers breach or potential breach of data privacy shall notify the DPO, through the Data Breach Notification form, of such incident. The DPO shall then report the incident to the DPT;
- b. A Privacy Breach Report shall be initiated for each incident of breach within 72 hours or three (3) business days of notification;
- c. In the event there is reasonable cause to believe that personal information has been disclosed to unauthorized parties, or is likely to be disclosed, further notification shall be given to:
 - i. The Department Secretary, in cases of High Severity of the breach which is greater than 100 data subjects and involves sensitive personal

information. Impact to data subject is high and may cause financial loss, discrimination, physical harm or harm to dignity, which may be irreversible, and that they may not overcome;

- ii. The Personal Information Controller;
- iii. Affected process owners or PIP so that the person to whom personal information applies can be notified about the breach; and,
- iv. The affected individuals, who may be internal or external data subjects.

3. Actions following breach of data privacy;

Upon discovery of a breach of privacy or potential breach of privacy, the following actions shall be taken:

- a. Employee to notify appropriate personnel;
 - i. The DPO shall be notified in all incidents of Data Privacy Breach activating the DBRT. The DBRT shall ensure immediate action in such event;
 - ii. The Department Secretary shall be notified by the DPO if the breach took place through theft, loss or unauthorized access to the Department's computer systems;
 - iii. ITMS shall be notified by the DPO if the breach took place through unauthorized access to computer systems;
 - iv. Security Division shall be notified by the DPO if the breach took place through unauthorized access to premises; and,
 - v. Notify concerned bureau/division where breach took place and affected data subjects if breach is indicative of process failure in the collection, use, transfer, retention or disposal of personal information.
- b. The DPO to assess the incident;
 - i. Determine the type of personal information involved, the volume of information, its format and its location;
 - ii. Determine likely cause of breach (whether intentional or accidental) ;
 - iii. Assess likelihood of disclosure of personal information to unauthorized parties or likelihood that it may be disclosed in the future; and,
 - iv. If there is reasonable cause to believe that personal information has or is likely to be disclosed to unauthorized parties, notify DOE Secretary and affected PIPs in question that a breach of privacy has occurred.
- c. The DPO to contain the breach;
 - i. Recover and secure personal information disclosed or may be disclosed. This may include gathering and shredding of manual forms, erasing files on laptops and so on.

- d. Data Privacy Committee to notify affected parties;
 - i. If there is reasonable cause to believe that personal data breach took place, efforts should be made to contact affected data subjects and inform them of the breach; and,
 - ii. Notify National Privacy Commission of the breach and seek direction on further actions.
 - e. The DPO to prepare Report of Breach;
 - i. Acquire template for Report of Breach from the Department's network folder for Data Privacy document archives and prepare report.
 - f. The DPO, alongside the DPC, to investigate and remediate the breach; and,
 - i. Investigate breach of data privacy; and,
 - ii. Breach report should contain information on the cause and/or reason for breach and recommendations for remediation measures to prevent similar breaches from occurring in the future.
 - g. The DPO, alongside the DPC, to complete the Privacy Breach Report.
 - i. Finalize Breach Report and obtain sign-off of the DPO; and,
 - ii. Upon sign-off, the DPO will distribute report to stakeholders involved and retain copy in the Data Privacy document archives.
4. Handling of Data Privacy Complaints; and,
- a. The Department shall investigate all complaints and will inform individuals who make inquiries or lodge complaints regarding personal information;
 - b. If complaint is deemed justified, The Department will take necessary actions to resolve complaints including, if necessary, amending the Manual;
 - c. In addition, an individual may file a complaint to the National Privacy Commission regarding issues on personal information processed by The Department;
 - d. The Department shall use a standard complaint form which will be available to the public via download from The Department's website;
 - e. The Data Protection Officer shall be notified about each complaint received and will notify appropriate parties, which may include the CEO/President and the National Privacy Commission;
 - f. All complaints shall be investigated in a timely manner. A Privacy Breach Report shall be prepared documenting results of investigation and recommendations to resolve the complaint. This report shall be provided to the complainant and related parties;
 - g. All documented complaints shall be retained in the Department's network folder containing Data Privacy document archives; and,

h. A Privacy Breach Report shall be reviewed and signed-off by the DPO.

5. Handling of Data Privacy Inquiries

- a. The Department will respond to all inquiries and will inform individuals who make inquiries of the inquiry process;
- b. A Standard Privacy Inquiry Form shall be used and made available to the public via download from The Department's website;
- c. All inquiries shall be responded in a timely manner. A Response Letter shall be prepared for each inquiry. The response shall be provided to the Data Protection Officer, the CEO/President and all related parties; and,
- d. All inquiries and responses shall be documented in log of Privacy Inquiries and retained in the Department's network folder for Data Privacy document archives containing the following information:
 - i. Unique inquiry identification number
 - ii. Date of inquiry
 - iii. Name of the person/s making the inquiry
 - iv. Summary of the nature of inquiry
 - v. Date of response
 - vi. Name of person making response
 - vii. Summary of response
 - viii. Copy of privacy Inquiry Form
 - ix. Copy of Response Letter

SECTION XII. ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

Principle of Accountability

Each Personal Information Controller is responsible for personal information under his/her control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

- a. The Personal Information Controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party; and,
- b. The Personal Information Controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

SECTION XIII. SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

1. *Responsibility of the Head of Agency*

All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the NPC. The head of the agency shall be responsible for complying with the security requirements while the NPC shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

2. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information*

- a. On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the agency; and,
- b. Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location of government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:
 - i. Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;
 - ii. Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and,
 - iii. Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be performed by the use of the most secure encryption standard recognized by the Commission.

3. ***Applicability to Government Contractors***

In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (1,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

SECTION XIV. PENALTY

1. The penalties in the DOE-Data Privacy Manual, insofar as they are not in conflict with the Data Privacy Act and other relevant laws, shall be adopted in this Department Order.

2. ***Extent of Liability***

If the offender is a public official and he or she is found guilty of acts penalized under Sections 27 (Improper Disposal of Personal Information and Sensitive Personal Information) and 28 (Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes) of the Data Privacy Act, he or she shall, in addition to the penalties prescribed therein, suffer perpetual or temporary absolute disqualification from office, as the case may be.

3. ***Offense Committed by Public Officer***

When the offender or the person responsible for the offense is a public officer as defined in the Administrative Code of the Philippines in the exercise of his or her duties, an accessory penalty of disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.

SECTION XV. SEPARABILITY CLAUSE

If any part of this Guidelines is declared unconstitutional or invalid by a court of competent jurisdiction, such decision shall not affect the validity of the remaining provisions of this Guidelines, or the Guidelines in its entirety.

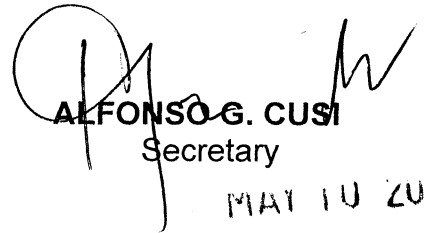
SECTION XVI. REPEALING CLAUSE

The DOE may amend or modify this Guidelines to maintain its future applicability. Any future amendments or modifications shall form part of the overall guidelines which will be considered binding on all end-users.

SECTION XVII. EFFECTIVITY

This Department Order shall take effect immediately upon its issuance and shall remain in full force and effect until sooner modified or revoked by the Secretary or any competent Authority.

Signed and approved on ____ day of _____ 2022 in Bonifacio Global City, Taguig City, Metro Manila.


ALFONSO G. CUSI
Secretary

MAY 10 2022



Republic of the Philippines
DEPARTMENT OF ENERGY
IN REPLYING PLS. CITE:

DOE-AGC-22002595



IV. Definition of Terms

Whenever used in this Guidelines, the following terms shall have the respective meanings hereafter set forth:

1. **Compliance Officer for Privacy or COP** - an individual or individuals who shall perform some of the functions of a DPO.
2. **Confidential information** – Refers to data or information which is not intended for general dissemination. Examples include proprietary technical information, disciplinary case records, administrative records, and the like.
3. **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. A personal data breach may be in the nature of:
 - An availability breach resulting from loss, accidental or unlawful destruction of personal data;
 - Integrity breach resulting from alteration of personal data; and/or
 - A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.
4. **Data Privacy Principles** – the processing of personal data shall be allowed subject to adherence to the principles of transparency, legitimate purpose, and proportionality.
5. **Data Processing Systems** - the structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing.
6. **Data Protection Officer** - an individual designated by the head of agency to be accountable for the agency's compliance with the Act: Provided, that the individual must be an organic employee of the government agency: Provided further, that a government agency may have more than one data protection officer.
7. **Data Protection Team** – a group of individuals whose aim is to assist the Data Protection Officer to observe his/her duties.
8. **Data Sharing** – the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller: Provided, that a personal information processor may be allowed to make such disclosure or transfer if it is upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of

personal data by a personal information controller to a personal information processor.

9. **Data Subjects** – an individual whose personal, sensitive personal, or privileged information is processed.
10. **De-identified or aggregated information** – These are information that do not have personal identified information e.g. statistical data, reports and all information required under the Freedom of Information
11. **Document** – Refers both to the paper and its electronic format.
12. **DOE** – The Department of Energy.
13. **DOE System** – This refers to the DOE Central Office and Field Offices ICT equipment, facilities, and information and communication systems.
14. **E-mail** – Electronically transmitted mail.
15. **Electronic document** – It refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically.
16. **Encryption** – A way to make data unreadable to everyone except the receiver.

This is done with the use of formula, called encryption algorithm. It translates plain text into an incomprehensible cipher text.
17. **ICT Administrator** – Refers to the person designated to manage the particular system assigned to her/him, to oversee the day-to-day operation of the system, or to preliminarily determine who is permitted access to particular facilities and resources of the ICT System, whether hired on a temporary, contractual or permanent basis.
18. **Information and Communications Technology System or ICT System** – Includes computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, and software, databases and other data files that are owned, managed, or maintained by DOE. For purposes of this Policy, any other equipment, computer unit or external network, when attached to, or used to access and/or interact with any component of, the IT System may also be considered part of the ICT System.
19. **Information** - Data, text, images, sounds, codes, computer programs, software, databases or similar items.

20. **Internet** – A system of linked computer networks, global in scope, that facilitates data communication services such as remote login, file transfer, electronic mail, and newsgroups. The internet is a way of connecting existing computer networks that greatly extends the reach of each participating system.
21. **Leased-line - Local Area Network (LAN)** – A network that connects computers in a small predetermined area like a room, a building, or a set of buildings. LANs can also be connected to each other via telephone lines, and radio waves. Workstations and personal computers in an office are commonly connected to each other with a LAN. These allow them to send/receive files and/or have access to the files and data. Each computer connected to a LAN is called a node.
22. **Legitimate purpose** – The process of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
23. **Litigation privilege** – Protects any document or communication between a lawyer, its client or a third party and is created for the dominant purpose of preparing for existing anticipated litigation.
24. **Network** – A communications system that links two or more computers. It can be as simple as a cable strung between two computers a few feet apart or as complex as hundreds of thousands of computers around the world linked through fiber optic cables, phone lines and satellites.
25. **Non-Disclosure Agreement** – a legally binding contract that establishes a confidential relationship. The party or parties signing the agreement agree that sensitive information they may obtain will not be made available to any others. An NDA may also be referred to as a confidentiality agreement.
26. **Non-DOE Personnel** – It refers to job orders, project partners, service contractors, and other stakeholders not employed by the DOE.
27. **Personal Data** – all types of personal information, including privilege communication.
28. **Personal Information** - any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.
29. **Personal Information Controller** - a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold,

process, use, transfer or disclose personal information on his or her behalf. The term excludes:

- A person or organization who performs such functions as instructed by another person or organization; and
- An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

30. **Personal Information Processing** - any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.
31. **Privacy Breach** – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.
32. **Privacy Impact Assessment** – a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system.
33. **Privacy Management Program** – a holistic approach to privacy and data protection, important for all agencies, companies or other organization involved in the processing of personal data.
34. **Privacy Manual** – serves as a guide or handbook for ensuring the compliance of an organization or entity with the DPA, its Implementing Rules and Regulations (IRR), and other relevant issuances of the National Privacy Commission (NPC). It also encapsulates the privacy and data protection protocols that need to be observed and carried out within the organization for specific circumstances (e.g., from collection to destruction), directed toward the fulfillment and realization of the rights of data subjects.
35. **Privacy Notice** – a statement made to a data subject that describes how the organization collects, uses, retains, and discloses personal information.
36. **Privacy Policy** – an internal document intended to explain to employees their responsibilities for ensuring compliance with the Data Privacy Act of 2012.
37. **Proportionality** – The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.
38. **Record** – Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and that is retrievable in perceivable form.

39. **Security Procedure** – A procedure that is used to verify that an electronic signature, record, or performance is that of a specific person; to determine that the person is authorized to sign the document; and, to detect changes or errors in the information in an electronic record. This includes a procedure that requires the use of algorithms or other codes, identifying words or numbers or encryption, callback or other acknowledgment procedures.
40. **Server** – A computer that provides a central service to a network, such as: storage of files (data server); location of application software (application server); e-mail services (e-mail server).
41. **Transaction** – An action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.
42. **Transparency** – The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
43. **Third-Party Service Agreement** – a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: Provided, that only personal information controllers shall be made parties to a data sharing agreement.
44. **Unit** - The DOE organization conducting business by means of an e-signature such as a bureau, services, office, or division.
45. **Wireless Access Point** - a device that provides a wireless local area network (WLAN) usually in an office or large building.
46. **Workstation** - A computer intended for professional or business use, and is faster and more capable than a personal computer. The applications intended to run in workstations are those used by design engineers, architects, graphic designers, and any organization, department, or individual that requires a faster microprocessor, larger amount of random access memory (RAM), and special features such as high-speed graphics adapters.