PNPC Circular Year-NO.

Date : **XX Month XXXX**

Subject : **Data Privacy and Protection Management System – Requirements under the Philippine Privacy Mark Certification Program**

WHEREAS, Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications in nation-building and its inherent obligation to ensure that personal data in information and communications systems in the government and the private sector are secured and protected.

WHEREAS, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes monitoring and ensuring compliance of the country with international standards set for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector.

WHEREAS, the NPC established the Philippine Privacy Mark (PPM) Certification Program, a voluntary certification program, to assess public and private organizations that implement data privacy and protection management systems, to ensure the secure and protected processing of personal information.

WHEREAS, the NPC issued NPC Circular 2023-05 which governs the pre-requisites for certification of personal information controllers (PICs) or personal information processors (PIPs) and accreditation of certification bodies (CBs) under the PPM Certification Program.

WHEREAS, the NPC issued NPC Circular 2024-XX which governs the requirements for CBs for the application and audit process of the PPM Certification Program.

WHEREAS, the NPC issued NPC Circular 2024-XX which governs the procedures for the certification of applicant organizations under the PPM Certification Program.

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the requirements for a Data Privacy and Protection Management System (DPPMS) under the PPM Certification Program.

SECTION 1. ***Scope.*** **-** This Circular specifies the requirements for establishing, implementing, maintaining, and continually improving a DPPMS within the determination or context of an organization under the PPM Certification Program.

It applies to all interested organizations, whether public or private, which are PICs and PIPs processing personal data, within the scope of the DPA.

SECTION 2. ***Definition of Terms.*** **–** The definition of terms in the DPA and its IRR, as amended, and NPC Circular 2024-XX (PPM Certification Scheme for CBs), are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. "Automated Decision-making" refers to a wholly or partially automated processing operation that can make decisions using technological means totally independent of human intervention; automated decision-making often involves profiling;
B. "Compliance Officer for Privacy" or "COP" refers to an individual that performs the functions or some of the functions of a DPO in a particular region, office, branch, or area of authority;
C. "Control Framework" refers to a set of security measures that is a comprehensive enumeration of the controls intended to address the risks, including organizational, physical, and technical measures to maintain the availability, integrity, and confidentiality of personal data and to protect it against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, or contamination;
D. "Data Center" refers to a centralized repository for the storage, management, and dissemination of data including personal data. This may be physical or virtual, analog or digital, or owned and controlled by the PIC or not;
E. "Data Protection Officer" or "DPO" refers to an individual designated by the head of agency or organization to ensure its compliance with the Act, its IRR, and other issuances of the Commission: Provided, that, except where allowed otherwise by law or the Commission, the individual must be an organic employee of the government agency or private entity: Provided further, that a government agency or private entity may not have more than one DPO;
F. "Data sharing" is the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controllers.
   In the case of a personal information processor, data sharing should only be allowed if it is carried out on behalf of and upon the instructions of the personal information controller it is engaged with via a subcontracting agreement. Otherwise, the sharing, transfer, or disclosure of personal data that is incidental to a subcontracting agreement between a personal information controller and a personal information processor should be excluded;
G. "Data Sharing Agreement" or "DSA" refers to a contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the personal information controllers involved in the transfer of personal data between or among them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the data subjects: provided, that only personal information controllers should be made parties to a data sharing agreement;
H. "Encryption" refers to the reversible transformation of data by a cryptographic algorithm to produce ciphertext in order to hide the information content of the data;
I. "Head of Agency" refers to:
   1. the head of the government entity or body, for national government agencies, constitutional commissions or offices, or branches of the government;

2. the governing board or its duly authorized official for government-owned and -controlled corporations, government financial institutions, and state colleges and universities;
3. the local chief executive, for local government units;

J. "Head of Organization" refers to the head or decision-making body of a private entity or organization;
For private organizations or government-owned and controlled corporations organized as private corporations, the Head of Organization may be the President, the Chief Executive Officer, or the Chairman of the Board of Directors or any officer of equivalent rank in the organization.

K. "Privacy Impact Assessment" or "PIA" is a process undertaken and used to evaluate and manage impacts on privacy of a particular program, project, process, measure, system or technology product of a PIC or PIP program, project, process, measure, system or technology product of a PIC or PIP. It takes into account the nature of the personal data to be protected, the personal data flow, the risks to privacy and security posed by the processing, current data privacy best practices, the cost of security implementation, and, where applicable, the size of the organization, its resources, and the complexity of its operations;

L. "Privacy-by-Design" refers to an approach to the development and implementation of projects, programs, and processes that integrate into the design or structure safeguards that are necessary to protect and promote privacy unto the design or structure of a processing activity or a data processing system;

M. "Security Incident Management Policy" refer to policies and procedures implemented by a personal information controller or personal information processor to govern the actions to be taken in case of a security incident or personal data breach;

N. "Threat" refers to a potential cause of an unwanted incident, which may result in harm or danger to a data subject, system, or organization;

O. "Vulnerability" refers to a weakness of a data processing system that makes it susceptible to threats and other attacks.

SECTION 3. ***Structure.*** **–** This document focuses on privacy-related requirements for management systems which are based on the applicable provisions of the DPA, its IRR, and other relevant issuances of the NPC and the requirements of ISO/IEC 27701: 2019.

Annex A contains the documented evidence for each clause requirement.

Annex B contains the Guidelines on Privacy Impact Assessment and the standard content of a PIA.

Annex C contains the required contents of a DSA.

Annex D contains the data protection control objectives, requirements, considerations, and guide questions for an organization processing personal data.

SECTION 4. Governance.

A. Determining the purpose and role of the organization. The organization shall consider its roles, functions, and services that relate to data processing to achieve the purpose of the DPPMS. It shall also consider the following:
    1. Role or roles of the organization as a PIC and/or PIP in the identified processing of personal data. In accordance with the CID 18-E-040, which states that "There is nothing in the law that requires entities to be engaged in the primary business of processing information before they are considered personal information controllers. By having the control of and discretion in the use of personal information of individuals, they are already considered the controller. They are thus accountable for the protection of the information and for the observation of the obligations under the law. These persons and entities must be able to justify their processing of personal data under any of the lawful criteria provided in the law. They have an obligation to provide mechanisms for the access, correction, and removal of personal data upon request, as well as the filing of a complaint. They are further required to secure the processing of any personal data by documenting and implementing organizational, technical and physical measures to respect the abovementioned rights. At the core of these obligations are the general data privacy principles of transparency, legitimate purpose, and proportionality.";
    2. Law and regulations in processing personal data; and
    3. The needs and expectations of relevant stakeholders.

B. Designating the Data Protection Officer. The organization shall designate an individual (or individuals) who shall function as data protection officer (DPO) or compliance officer (COP) and will be accountable for ensuring conformity with this document's requirements and applicable regulatory requirements for data privacy and protection. The designation shall be formalized and made available through a written and notarized document. For a more detailed guidance on the designation of DPO, kindly refer to Annex A.

C. Defining the scope of the data privacy and protection management system. The organization shall determine the extent and limitations of the data privacy and protection management system. In determining the scope, the organization shall consider the following:
    1. the requirements indicated in this document;
    2. the purpose(s), process(es) and role(s) of the organization referred in 1.1;
    3. the applicable privacy legislation and regulations;
    4. the applicable judicial decisions; and Commission en Banc decisions;
    5. the applicable contractual requirements and obligations;
    6. the statement of applicability of controls.

    The identified scope shall be made available as documented information.

D. Registration with the National Privacy Commission. The organization shall register its DPO and data processing systems or records of processing activities with the National Privacy Commission based on the latter's registration process and issuances.

SECTION 5. Data Privacy Risk Management.

A. Determining the organization's personal data processing systems and activities. Section 26(c) of the IRR states that any natural or juridical person or other body involved in the processing of personal data shall maintain records that sufficiently describe its data processing system and identify the duties and responsibilities of those individuals who will have access to personal data.

   In determining its assets for personal data processing systems and activities, the organization shall consider the purpose(s) and need(s) identified in Section 4A, and maintain records or inventory that describes its personal data processing systems and activities.

   The records or inventory shall be accurate, up to date, and consistent. It shall include the following details:

   1. Purpose/s of the personal data processing systems or activities;
   2. Description of all categories of data subjects, personal data, and data recipients;
   3. Description of each lifecycle stage within and outside the organization; and
   4. Process owners of the identified personal data processing systems or activities.

B. Conduct of Privacy Impact Assessments. Section 20(c) of the DPA states that the determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices and the cost of security implementation.

   The organization shall define and conduct the privacy impact assessments of all the identified personal data processing systems and activities in 2.1. Refer to Annex B, which contains the Guidelines in Conducting a Privacy Impact Assessment, when performing a PIA.

   As a supplement, the organization may also refer to NPC Advisory 17-03 (Guidelines on Privacy Impact Assessments).

   Upon the conduct of the privacy impact assessment, the organization shall produce a Statement of Applicability that contains the necessary controls (Annex D) and justification for inclusions, whether they are implemented and the justification for exclusions of controls.

C. Personal Data Lifecycle.

   1. General. Section 19 of the IRR states that the processing of personal data shall adhere to the following general principles in the collection, processing and retention of personal data.

      During the conduct of the PIA and based on its results, the organization shall determine its personal data processing systems and activities that process data at each stage of the personal data lifecycle.

   2. Collection. The organization shall ensure that the collection of personal data in each identified personal data processing system or activity is in accordance with Section 11 of the DPA of 2012, which states that the processing of personal information shall be allowed, subject to compliance with the requirements of this ACT and other laws allowing disclosure of information to the public and adherence to the principle of transparency, legitimate purpose, and proportionality, and Section 12 and 13 for the Criteria for Lawful Processing of Personal Information, Sensitive Personal Information, and Privileged Information.

3. Usage. The organization shall ensure that the use of personal data in each identified personal data processing system or activity is lawful and proportional to its defined purpose(s) and need(s).
4. Storage and Retention. The organization shall ensure the protection of personal data stored in its personal data processing systems, products, and services. It shall determine the appropriate retention periods that apply to different types of processing or categories of personal data and considerations for relevant laws and regulations. For example, government agencies are regulated by the requirements of the National Archives of the Philippines (NAP). Likewise, best practices from different industry standards should be considered.
5. Disclosure and Transfer. The organization shall identify the relevant basis of disclosure and transfers of personal data between jurisdictions or third parties.
6. Disposal and Destruction. The organization shall have policies, procedures, and measures on the disposal and destruction of personal data.

   The organization shall retain documentation that shows the personal data lifecycle for each data processing system or activity and shall be reflected in the records of processing activities.

   Identifying data flow involved in the data processing system or activity is one of the activities when conducting PIA. Hence, having documentation for the personal data lifecycle for each data processing system or activity will be helpful when an organization conduct PIA.

D. Privacy-by-Design and Privacy-by-Default.
   1. General. The organization shall apply privacy-by-design and privacy-by-default approach on its personal data processing systems and activities and other projects/programs that involve personal data processing by adhering to the data privacy principles and incorporating the data protection principles.
   2. Data Privacy Principles. Section 11 of the DPA and Section 17 of the IRR state that the processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

      The organization shall ensure that all identified personal data processing systems, products, services, programs, and projects adhere to the following data privacy principles:

      a. Transparency. The organization shall ensure that the identified personal data processing systems, activities, programs, and projects adhere to openness and transparency, providing the data subjects with clear, concise and understandable information about the organization's purpose(s) and need(s) for processing personal data.

         The organization has to examine whether an average member of the target audience could have understood the information provided to them. Transparency requirement means that the information required under Sections 18(a) and 34(a)(2) of the Implementing Rules and Regulations should be provided in as simple a manner as possible and it should not be phrased in abstract or ambivalent terms or leave room for different interpretations.

         The organization shall take into consideration the targeted data subjects in drafting and presenting the privacy notices or any related information on the

transparency of the personal data processing systems. This is in accordance with NPC Decision 19-498.

b. Legitimate Purpose. The organization shall ensure that the processing of data in each identified personal data processing systems, activities, programs, and projects is compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.

c. Proportionality. The organization shall ensure that the identified personal data processing systems, activities, programs, and projects act on appropriate and proportional amount of personal data, limited only to the specified purposes.

3. Data Protection Principles. Section 25 of the IRR states that the security measures shall aim to maintain the availability, integrity, and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

   Also, Section 28(c) of the IRR states that where appropriate, the personal information controllers and personal information processors shall adopt and establish technical measures including the ability to ensure and maintain the confidentiality, integrity, and availability, and resilience of their processing systems and services. The organization shall preserve the confidentiality, integrity, and availability of personal data that are being acted upon by the personal data processing systems, activities, programs, and projects by applying appropriate data privacy risk management processes.

   The organization shall consider these principles in implementing risk treatments, measures, and recommendations.

E. Determining Security Incident Management Policy.

1. General. The organization shall implement a consistent and effective approach to identify, record, and manage security incidents, including personal data breach. Management and employees' responsibilities shall be established to ensure quick and effective response to incidents.

2. Data Breach Response Team. The organization shall constitute a data breach response team responsible in implementing the security incident management policy of the organization. See Section 5 of NPC Circular 16-03.

3. Security Incident Management Procedures. The organization's security incident management policy shall include data protection measures intended to prevent or minimize the occurrence of a personal data breach.

   The measures shall also ensure the confidentiality, integrity, and availability of the personal data being processed.

   a. Responsibilities, roles and procedures. The organization shall establish the roles and responsibilities to ensure a responsive, effective, and systematic response to any security incidents.

   b. Reporting security incident events. The organization shall establish reporting procedures on different channels or outlets, ensuring the Data Breach Response Team's appropriate and immediate response procedures to address security incidents.

   c. Reporting security vulnerabilities and threats. The organization shall establish reporting procedures of vulnerabilities and potential threats from internal and

external stakeholders using the processes and systems within the DPPMS to the Data Breach Response Team.

d. Assessment, investigation and identification of security incidents. Section 28(d) of the IRR states that where appropriate, personal information controllers and personal information processors shall adopt and establish technical measures including regular monitoring for security breaches, and a process both for identifying and accessing reasonably foreseeable vulnerabilities in their computer networks, and for taking preventive, corrective, and mitigating action against security incidents that can lead to a personal data breach.

   The organization shall establish procedures to assess, investigate, and identify security incidents to classify and categorize them based on its potential impact.

e. Response procedures. The organization shall establish procedures to respond efficiently to the identified security incident.

   In accordance with NPC Decision 19-067, the incident response procedures objectives are to investigate and contain the security incident and restore the integrity to the affected personal data processing systems. The investigation shall provide in-depth procedures of the security incidents that should determine the cause and possible effects to both organizations and data subjects.

f. Learning from security incidents. The organization shall document the knowledge learned from analyzing and resolving security incidents for future reference.

4. Incident Documentation.

   a. General. Section 41(b) of the IRR states that all security incidents and personal data breaches shall be documented through written reports, including those not covered by the notification requirements. In the case of personal data breaches, a report shall include the facts surrounding an incident, effects of such incident, and the remedial actions taken by the personal information controller. In other security incidents not involving personal data, a report containing aggregated data shall be made available when requested by the Commission.

      The organization shall document all actions taken by the concerned employees and the data breach response team. The report must include the following information:

      1) a description of the security incident or personal data breach, specifically its root cause and the circumstances surrounding its discovery and occurrence;
      2) actions and decisions taken by the data breach response team;
      3) outcome of the security incident management and the challenges encountered; and
      4) fulfillment of notification requirements and assistance provided to the data subjects.

   b. Regular Review. The organization shall establish a process to review the breach or security incident after it has occurred to further improve the security incident management policies and procedures.

5. Notification Procedures. Section 20(f) of the DPA states that the PIC shall promptly notify the Commission and affected data subjects when sensitive personal

information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes (bat such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and the measures taken by the entity to address the breach.

Also, Section 38(a) of the IRR states that the Commission and affected data subjects shall be notified by the personal information controller within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the personal information controller and personal information processor that, a personal data breach requiring notification has occurred.

Also, Section 39 of the IRR states that the notification shall at least describe the nature of the breach, the personal data possibly involved, and the measures taken by the entity to address the breach.

The organization shall establish procedures or criteria to determine when to notify the National Privacy Commission, the affected data subjects, and other government and/or regulatory agencies.

The organization shall ensure that all reasonable mechanisms in notifying all affected data subjects are made aware of the breach. The mechanisms should guarantee that the notification they sent to the data subjects has been received. The requirements are in accordance with NPC BN 20-157.

The organization must include the following in its notification to the National Privacy Commission and other government and/or regulatory agencies:

a. nature of the breach or incident;
b. description of personal data that may possibly be involved; and
c. measures taken to address the breach or security incident.

The organization must include the following in its notification to the data subjects:

a. nature of the breach or incident;
b. description of personal data that may possibly be involved;
c. measures taken to address the breach or security incident; and
d. measures taken to reduce the harm or negative consequences of the breach.

In accordance to NPC BN 17-021, the risks and harms that data subjects may face from a security incident or personal data breach shall be viewed holistically taking into consideration all the relevant circumstances. It may even include risks and harms that are outside the control of the organization's personal data processing system that was breached.

The requirements in Section 4E are related to the data protection control objectives, requirements, considerations, and guide questions in Annex D.

NPC Circular 16-03 is the NPC issuance on personal data breach management which relates to Section 4E.

F. Third Party Management.
   1. General. Section 21 of the DPA states that each personal information controller is responsible for personal information under its custody, including information that have been transferred to a third-party processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

Also, Section 44 of the IRR states that the processing by a personal information processor shall be governed by a contract or other legal act that binds the personal information processor to the personal information controller.

The organization shall ensure the data protection of its personal data processing systems, activities, programs, and projects that are accessible to third parties.

2. Data sharing agreement. Section 20 of the IRR states that the further processing of personal data collected from a party other than the data subject shall be allowed under the given conditions. The NPC Circular 2020-03 provides the guidelines and requirements on data sharing agreements.

   Personal data that are shared between two or more PICs may be governed by a DSA. The organization shall determine the roles and responsibilities on personal data processing which include the data protection requirements of the other PIC following the accountability principle stated in Section 12 of the NPC Circular 2020-03.

   The requirements here in Section 4F2 relate to the required contents in Annex C.

3. Subcontracting. Section 43 of the IRR states that a personal information controller may subcontract or outsource the processing of personal data: Provided, that the personal information controller shall use contractual or other reasonable means to ensure the proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the Act, these Rules, other applicable laws for processing of personal data, and other issuances of the Commission.

   The organization shall establish in its subcontracting agreement with a third party, its requirements in the third party's conduct of personal data processing. The applicable provisions in Section 44 of the IRR on the elements of a DSA shall also be followed for the subcontracting agreement.

G. Data Subjects' Rights. Section 16, 17 and 18 of the DPA and Section 34 of the IRR state the rights that a data subject is entitled to.

   The organization shall document the fulfillment of its legal, regulatory, and business obligations to the data subjects that are related to processing of their personal data. The data subjects shall be provided with sufficient details about the processing of their personal data and procedures on how to exercise their rights that adhere to Section 4D.

H. Establishment of Privacy Management Program and Privacy Policy.

1. General. The organization shall address the risks identified in the PIA by a control framework, which is a comprehensive enumeration of the measures, treatments, and recommendations intended to address the risks. It shall be included in the organization's privacy management program and privacy manual.
2. Privacy Management Program. Section 20(a) of the DPA states that the personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

   Also, Section 25 of the IRR states that personal information controllers and personal information processors shall implement reasonable and appropriate

organizational, physical, and technical security measures for the protection of personal data.

The organization shall compile and ensure the proper implementation of the management-approved measures, treatments, and recommendations created to address the risks/gaps found during the conduct of the PIAs.

The PMP shall be made available as a documented information.

3. Privacy Policy. Section 16(b) of the DPA states that the data subject is entitled to be furnished the information hereunder before the entry of his or her personal information into the processing system of the personal information controller.

   Section 26(b) of the IRR states that any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedom of data subjects.

   Section 34(a) of the IRR states that the right of the data subjects 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.

   The organization shall establish a Privacy Policy that governs how the organization processes personal data. It aims to inform its employees about the proper use of personal data, rights of the data subjects, and the implementation of appropriate data protection measures.

   The Privacy Policy shall be made available as a documented information.

4. Privacy Manual. Section 26(b) of the IRR states that any natural or juridical person or other body involved in the processing of personal data shall implement appropriate data protection policies that provide for organization, physical, and technical security measures, and for such purpose, take into account the nature, scope, context and purposes of the processing, as well as the risks posed to the rights and freedom of data subjects.

   The organization shall establish and maintain a manual of procedures to operationalize the measures, treatments, and recommendations included in the PMP.

   The organization shall keep the privacy manual up to date. It may produce both internal and external versions of the manual – the former for employees use and the latter for reference of the data subjects.

SECTION 6. Operational Implementation.

A. Operationalizing the Privacy Manual. The organization shall plan and implement the measures, treatments, and recommended solutions compiled in subclause 2.8.2 to control its processes and personal data processing systems, activities, programs, and projects and meet the DPPMS requirements.

B. Communication of privacy manual.

   1. General. The organization shall circulate and properly communicate the privacy manual to its employees involved in personal data processing.

      Relevant to the DPPMS, the organization shall determine the need for internal and external communications which may include the following:

      a. communication message;

b. timing of communication;
c. target audience of the communication;
d. employees responsible for the communication;
e. platform/s of communication; and
f. processes by which the communication shall be effected.

2. Employee Awareness. Regarding DPPMS, the employees of the organization shall be aware of the organization's policies, their roles and responsibilities, and the implications of non-conformity with the DPPMS requirements.

C. Privacy Notice.

1. General. The organization shall identify situations where providing notice is necessary, considering the information determined in Sections 5B and 5C. The notice provided should comply with the requirements in Section 6B2.
2. Contents of a privacy notice. Section 16(b) of the DPA of 2012 states that the data subject is entitled to be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

   Section 34(a)(2) if the IRR provides what information should be provided to data subjects.

   a. Description of the personal information to be entered into the system;
   b. Purposes for which they are being or are to be processed;
   c. Scope and method of the personal information processing;
   d. The recipients or classes of recipients to whom they are or may be disclosed;
   e. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized;
   f. The identity and contact details of the personal information controller or its representative;
   g. The period for which the information will be stored; and
   h. The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

   Section 34(a)(2) of the IRR states the right of the data subject to be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:

   a. Description of the personal data to be entered into the system;
   b. Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
   c. Basis of processing, when processing is not based on the consent of the data subject;
   d. Scope and method of the personal data processing;
   e. The recipients or classes of recipients to whom the personal data are or may be disclosed;
   f. Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
   g. The identity and contact details of the personal information controller or its representative;

h. The period for which the information will be stored; and
i. The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

Through the privacy notice, the organization shall provide the data subject with sufficient information to understand its personal data processing and their rights.

For the online services of the organization, it shall comply with the content requirements stated in ISO/IEC 29184 – Online privacy notices and consent:

a. purpose description;
b. presentation of purpose description
c. identification of the PIC;
d. personal data collection;
e. timing and location of the personal data collection;
f. method of use;
g. geo-location of, and legal jurisdictions over stored personal data;
h. third-party transfer;
i. retention period;
j. participation of data subjects;
k. inquiry and complaint;
l. information about accessing the choices made for consent;
m. basis for processing; and
n. risks

The organization shall also include the effectivity date of the privacy notice.

For non-online services, the organization shall specify the following details on its privacy notice:

a. description of the purpose;
b. identity of the personal information controller;
c. information on the elements of the personal data being collected;
d. method(s) of data processing (collection, usage, storage/retention, disclosure/transfer, and disposal/destruction);
e. third-party relationship;
f. data subjects' rights;
g. complaint procedure;
h. possible risks and measures; and
i. information on the effectivity date of the privacy notice.

D. Data Protection Measures. The organization shall implement data protection measures to address the risks identified during the conduct of the PIA and the requirements in Section 5B, including the organizational, physical, and technical measures to preserve the availability, integrity, and confidentiality of personal data and to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

Annex C contains a list of DPPMS requirements, considerations, and guide questions for DPPMS. Users of this document are directed to Annex C to ensure that no essential physical and technical controls are neglected.

E. Operational Competence. The organization shall determine and define the required competence of its employees that affect its DPPMS.

The organization shall ensure that its employees are competent or have gone through competency programs in handling its personal data processing products, services, systems, programs, and projects.

SECTION 7. Continuous Improvement.

A. Continuous DPPMS improvement. The organization shall continually improve the adequacy and effectiveness of its DPPMS.
The organization shall conduct a regular review of its PMP and other privacy policies, particularly whenever a PIA is conducted, to identify their effectiveness and/or challenges, evaluate the need for action to eliminate causes of non-conformity and prevent them from recurring or occurring somewhere else.
As stated in NPC Advisory 2017-03, a PIA "should be conducted for both new and existing systems, programs, projects, procedures, measures, or technology products that involve or impact processing personal data. For new processing systems, it should be undertaken prior to their adoption, use, or implementation. Changes in the governing law or regulations, or those adopted within the organization, or its industry may likewise require the conduct of a PIA, particularly if such changes affect personal data processing."

B. Internal audit
   1. General. The organization shall conduct internal audits regularly to provide information on whether the DPPMS conforms with its own identified requirements and the requirements of this document.
   The internal audit shall validate the implementation, maintenance, effectivity, and effectiveness of the DPPMS.
   The organization shall plan, establish, and maintain an audit program with requirements, criteria, and scope, including frequency, process responsibilities, planning requirements and reporting.
   2. Internal Audit Team. The organization shall constitute an internal audit team responsible for implementing security incident management within the organization.
   The internal audit team shall submit its findings and recommendations to the organization's top management for review and approval.
   All actions taken by the internal audit team shall be documented.
   3. Review of the management. The organization's top management shall review the audit findings and recommendations and decide on approval for implementation.
   4. Monitoring and Evaluation. The organization shall monitor and evaluate the implementation and the efficacy of its data privacy controls and security measures documented in Section 5H2.

C. Determining new applicable technologies and legal requirements. The organization shall regularly determine new legal and technological requirements that may affect its personal data processing systems, activities, products, services, programs, and projects.
The organization shall have knowledge management of applicable technology and legal requirements that supports continual improvement.

Approved:

JOHN HENRY D. NAGA
Privacy Commissioner

LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

NERISSA N. DE JESUS
Deputy Privacy Commissioner

Annex A – Documented Evidence for DPPMS

The table below contains the documented evidence for each clause in DPPMS that enables the organizations to demonstrate their conformance to the requirements.

1. Governance
1.1 Determining the purpose and role of the organization
Objective: The organization shall consider its roles, functions, and services that relate to data processing in order to achieve the purpose of the DPPMS.
Documented Evidence • Organizational Chart • General Information Sheet (GIS) • Agency Charter (For public sector) • Overall Privacy Policy • Organization's Data Privacy and Protection Management (DPPMS) Objective Documentation • SWOT Analysis or Assessment Activities identifying internal and external needs of the organizations for DPPMS
1.2 Designating the Data Protection Officer
Objective: The organization shall designate an individual (or individuals) who shall function as data protection officer (DPO) or compliance officer (COP) and will be accountable for ensuring conformity with this document's requirements and applicable regulatory requirements for data privacy and protection.
Documented Evidence • Office order of company issuance designating the DPO • Published contact details of the DPO through privacy notices, websites, etc.,
1.3 Defining the scope of the data privacy and protection management system
Objective: The organization shall determine the extent and limitations of the data privacy and protection management system.
Documented Evidence • Scope of Applicability of DPPMS requirements
1.4 Registration with the National Privacy Commission
Objective: The organization shall register its DPO and data processing systems or records of processing activities with the National Privacy Commission based on the latter's registration process and issuances.
Documented Evidence • Notarized DPO Form

- Data Processing System/Records of Processing Activities application form
- Certificate of Registration from NPC

2. Data Privacy Risk Management

2.1 Determining the purpose and role of the organization

Objective: In determining the organization's assets for personal data processing systems and activities, it shall consider the purpose(s) and need(s) identified in Clause 1.1 and maintain records or inventory that describes its personal data processing systems and activities.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Records or inventory of organization's data processing systems or activities
- Personal data inventory

2.2 Conduct of Privacy Impact Assessments

Objective: The organization shall define and conduct the privacy impact assessments of all the identified personal data processing systems and activities in Clause 2.1.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Privacy Impact Assessment Report *(Refer to Annex B for the guidelines in conducting a PIA)*
- Statement of Applicability - a document that contains a list of appropriate and necessary controls to address and mitigate identified risks, justification for inclusions, and whether the controls are implemented or not *(Similar with the ISO/IEC 27001 statement of applicability)*
- Policy that determines when to conduct risk assessments activities
- Threshold analysis *(Refer to NPC Privacy Toolkit 3rd Edition for sample PIA threshold analysis)*

2.3 Personal Data Lifecycle

Objective: During the conduct of PIA and based on its results, the organization shall determine its personal data processing systems and activities that process data at each stage of the personal data lifecycle.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Records or inventory of data processing systems or activities – a repository of all data processing systems or activities of the organization *(Refer to Clause 2.1 of this document for the detailed contents)*
- Personal data inventory – a record of categories of personal data processed by the organization

- Personal data flow diagram or mapping – complementary to the personal data inventory, it maps out the flow of personal data (e.g., considering the data lifecycle) involved in any process or system

2.3.2 Collection

Objective: The organization shall ensure that the collection of personal data in each identified personal data processing system or activity is lawful and with legal basis as per jurisdiction and national regulations

Documented Evidence:

- Policy on the collection of personal data, approved by the top management
- Privacy Notice in website, other platform and within organization's premise where collection occurs
- If applicable, consent form

2.3.3 Usage

Objective: The organization shall ensure that the use of personal data in each identified personal data processing system or activity is lawful and proportional to its defined purpose(s) and need(s).

Documented Evidence:

- If applicable, consent form
- Access control policy, approved by the top management
- Usage policy that includes the lawful basis for processing personal data, approved by the top management

2.3.4 Storage and Retention

Objective: The organization shall ensure the protection of personal data stored in its personal data processing systems, products, services and determine the appropriate retention periods.

Documented Evidence:

- Data center and storage area with limited access
- Retention policy that includes the determination of applicable laws and regulations on retention periods, approved by the top management

Useful standard in relation to storage – ISO/IEC 27040:2015 Information technology – Security techniques – Storage security

2.3.5 Disclosure and Transfer

Objective: The organization shall identify the relevant basis of disclosures and transfers of personal data between jurisdictions or third parties.

Documented Evidence:

- Policy on disclosure and transfer of personal data, approved by the top management
- Appropriate agreements or contracts for disclosure and transfer – *Refer to third party management*

2.3.6 Disposal and Destruction

Objective: The organization shall have policies, procedures, and measures on the disposal and destruction of personal data.

Documented Evidence:

- Disposal policy, approved by the top management

2.4 Privacy-by-Design and Privacy-by-Default

Objective: The organization shall apply privacy-by-design and privacy-by-default approach on its personal data processing systems and activities and other projects/programs that involve personal data processing by adhering to the data privacy principles and incorporating the data protection principles.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Privacy Impact Assessment for new and existing data processing systems and activities of the organization
- Privacy Management Program of the organization, approved by the top management
- List of programs, activities, initiatives of the organization that supports privacy-by-design and privacy-by-default
- Privacy-by-design operational model
    - List of employees responsible in operationalizing privacy-by-design for process development. This includes their activities and tasks.
    - Documentation of each or all systems and business process subject to privacy-by-design initiative including each of their lawful basis for personal data processing
        - Architectural representation of each or all systems and business process
        - Documentation of domains with each process owner
        - Personal Data Lifecyle of all systems and business process
        - Personal Data Inventory of each and all systems and business process
        - Documentation of privacy controls required within the use cases of each or all systems and business process
- If applicable, software development methodology for creating software applications
- If applicable, software application selection policy when procuring software applications
- Software manual

2.5 Determining Security Incident Management Policy

Objective: The organization shall implement a consistent and effective approach to identify, record, and manage security incidents, including personal data breach.

2.5.2 Data Breach Response Team

Objective: The organization shall constitute a data breach response team responsible in implementing the security incident management policy of the organization.

Documented Evidence

- Employees/Office Order or similar document that constitute the organization's Data Breach Response Team
- Documented information of the roles and responsibilities of the Data Breach Response Team

2.5.3 Security Incident Management Procedures

Objective: The organization's security incident management policy shall include data protection measures intended to prevent or minimize the occurrence of a personal data breach.

Documented Evidence

- Security incident response policy and procedures, with the consideration of guidelines stipulated in NPC Circular 16-03 Rule IV section 8.

2.5.3.1 RESPONSIBILITIES, ROLES AND PROCEDURES

Objective: The organization shall establish the roles and responsibilities to ensure a responsive, effective and systematic response to any security incidents.

Documented Evidence

- Office order or company memorandum designating the Data Breach Response Team members, their roles and responsibilities
- Security Incident Management Policy, approved by the top management

2.5.3.2 Reporting security incident events

Objective: The organization shall establish reporting procedures on different channels or outlet as efficient as possible.

Documented Evidence

- Reporting procedure policy of the Data Breach Response Team that includes internal reporting and external reporting

Internal – concerned office(s), top management

External – relevant regulatory agencies, affected data subjects

2.5.3.3 Reporting security vulnerabilities and threats

Objective: The organization shall establish reporting procedures of vulnerabilities and potential threats from internal and external stakeholders using the processes and systems within the DPPMS to the Data Breach Response Team.
Documented Evidence • Internal and External reporting procedures to the Data Breach Response team *Internal – e.g., concerned office(s), top management* *External – e.g., relevant regulatory agencies, affected data subjects*
2.5.3.4 Assessment, investigation and identification of security incidents
Objective: The organization shall establish procedures to assess, investigate and identify security incidents to classify and categorize them based on its potential impact.
Documented Evidence • Criteria in assessing reported security incidents • Investigation procedures of security incidents • Identification of roles and responsibilities of assigned personnel for the investigation • Security incident detection policy, approved by the top management
2.5.3.5 Response procedures
Objective: The organization shall establish procedures to response efficiently to the identified security incident.
Documented Evidence • Security incident response policy, approved by the top management • Documented response to an identified security incident
2.5.3.6 Learning from security incident
Objective: The organization shall document the knowledge learned from analyzing and resolving security incidents for future reference.
Documented Evidence • Compilation of Documented responses to identified security incidents • Updates/revision of security incident management policy based on the documented responses to security incidents
2.5.4 Incident documentation
Objective: The organization shall document all actions taken by the employees and the data breach response team. The report must include the following information:
Documented Evidence • Data Breach Report following the requirements stipulated in clause 2.5.4.1 • Record of security incidents and personal data breaches • Documented information on the conduct of regular review of security incident management policies and procedures

- Documented information on the notification procedures to NPC and/or relevant regulatory agencies
- If applicable, documented evidence or proof that the organization provided notification or report to the NPC and data subjects.

2.6 Third Party Management

Objective: The organization shall ensure the data protection of its personal data processing systems, activities, programs, and projects that are accessible to third parties.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Data Sharing Agreements
- Subcontracting Agreements
- List or inventory of recipients of personal data (e.g., PIPs, other PICs, service providers)

Note: Agreements with other PICs may follow the requirements stated in Annex C – Content requirements – Data Sharing Agreements

2.7 Data Subject's Rights

Objective: The organization shall document the fulfillment of its legal, regulatory, and business obligations to the data subjects that are related to processing of their personal data.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- Presence of Privacy Notice in website and other platform or location where the collection of personal data occurs
- Mechanisms or platform for data subjects to exercise their rights where appropriate including right to object, access, correction, erasure or blocking, data portability, right to damages
- Mechanisms or procedures for data subjects to file a complaint
- Policies and procedure in dealing with requests for information from parties other than the data subjects (e.g., media, law enforcement, other government representatives)
- Procedure for addressing complaints of data subjects

2.8 Establishment of Privacy Management Program and Privacy Policy

Objective: The organization shall address the risks identified in the PIA by a control framework, which is a comprehensive enumeration of the measures, treatments and recommendations intended to address the risks.

Documented Evidence

To demonstrate the organization's conformance to this clause, the following documented evidence shall be made available:

- List of measures, controls, treatments, and recommendation to address risks and gaps identified in the conduct of PIA
- Documented information on the management sign-off or approval of the measures and controls
- List of identified activities or programs on privacy and data protection
- Designation or assignment of key employees responsible for privacy and data protection efforts within the organization
- Privacy Policy, approved by the top management
- Organization's Privacy Manual, approved by the top management

3. Operational Implementation

3.1 Operationalizing of privacy manual

Objective: The organization shall circulate and properly communicate the privacy manual to its employees involved in personal data processing.

Documented Evidence

- Office order or Company Memorandum communicating and distributing the approved privacy management program and privacy manual to its employees. The office order or company memorandum shall include the details specified in Clause 3.2.1

3.2 Communication of privacy manual

Objective: The employees shall be aware of the organization's policies, their roles and responsibilities, and the implications of non-conformity with its requirements.

Documented Evidence

- Approved Communication plan for employees of the privacy manual
- Annual schedule or work plan of seminar/trainings for the implementation of the privacy manual
    - *Seminars/trainings for each employee shall be done at least annually.*
- Attendance of conducted seminar/trainings for the implementation of the privacy manual

3.3 Privacy Notice

Objective:

The organization shall provide the data subject with sufficient information to understand its personal data processing and their rights.

Documented Evidence

- Privacy notices for each processing activities

3.4 Data Protection Measures

Objective: The organization shall implement data protection measures to address the risks identified during the conduct of the PIA and requirements in subsection 2.2, including organizational, physical, and technical measures to preserve the availability, integrity, and confidentiality of personal data and protect the personal data against natural dangers such as accidental loss or destruction and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination.

Documented Evidence

- Physical Security Measures:
  - Perimeter Security
    - Physical Security Policy
    - Security Staffs Duties and Responsibilities
    - Visitor's Logbook
    - Office/Room and Cabinet Key Inventory
  - Policy for offices, rooms and facilities
    - Clear Desk Policy
    - Access Control Policy
  - Data protection against environment threats
    - Business Continuity Plan
  - ICT Asset Management
    - Asset management policy
    - ICT Inventory
  - Mobile Device Equipment
    - Mobile device policy which includes mobile phones, USB, drives, Laptops, External hard drives
  - Disposal or re-use of ICT assets
    - Disposal Policy for ICT Assets
    - ICT Repurposing Policy
- Technical Security Measures
  - User access management policy
  - Encryption policy
  - Authentication Policy for internal and external
    - Record of employees
    - Periodic review of the access rights of registered users
  - Authorization Policy for internal and external
    - List of user ids and their privileges
    - User Removal policy
  - Password management policy
  - Capacity management policy
  - Digital data assets management policy
  - Data masking/redaction/ of digital and physical documents
  - Data leakage prevention policy
  - Monitoring of activities policy
  - Software application management policy
  - Network security policy
  - Security incident management policy
    - Data Breach Response Team Designation document
    - Incident Response Procedures
    - List of contact information of authorities

- Templates of security incident report
- Annual security report

- Cloud management policy

- Security Clearance Policy
  - Personal Data Access Request Form
- Telecommuting policy and operations. It shall consider the following:
  - Authorized ICT Assets
  - Office-issued devices
  - Acceptable Use
  - Access Control
  - User Authentication and Authorization
  - Network Security
  - Records and File Security
  - Email and Online Communication
  - Continuity and Security Incident Management

3.5 Operational Competence

Objective: The organization shall determine and define the required competence of its employees that affect its DPPMS.

Documented Evidence

- Criteria of competence requirements for hiring employees
  - Relative knowledge and experience with the specific personal data processing that will be assigned;
  - Continual improvement methodologies and framework such as suggesting and analyzing corrective actions on process;
  - Analyze business impacts of emerging technologies on the assigned personal data processing; and
  - Understand and determine the scope of legal, regulatory, business and guideline requirements that may impact the personal data process and DPPMS requirements.
- Program plans to enhance the competence of employees
- List of trainings for data privacy and data protection offered to employees

4. Continuous Improvement

4.1 Continuous DPPMS improvement

Objective: The organization shall continually improve the adequacy and effectiveness of its DPPMS.

Documented Evidence

- Privacy Policy
- Policy on the conduct of internal audit
- Internal Audit Committee

4.2 Internal audit

Objective: A provision in the organization's privacy policy that mandates the conduct of internal audit to periodically check whether the DPPMS conforms to the implementation, maintenance, and effectiveness set by the DPPMS Criteria Document
Documented Evidence • Privacy Policy • Official order or any similar document to conduct internal audit
4.2.1 General
Objective: The organization shall conduct internal audits regularly to provide information on whether the DPPMS conforms to its own identified requirements and the requirements of this document.
Documented Evidence: • Privacy Policy • Official order or any similar document to conduct internal audit
4.2.2 Internal Audit Team
Objective: The organization shall constitute an internal audit team responsible for implementing security incident management within the organization.
Documented Evidence: • Privacy Policy • Official Order or any similar document constituting an internal audit team/designating employee as part of the internal audit
4.2.3 Review of the management
Objective: The organization's top management shall review the audit findings and recommendations and decide on approval for implementation.
Documented Evidence: • Privacy Policy • Internal Audit Report
4.2.4 Monitoring and Evaluation
Objective: The organization shall monitor and evaluate the implementation and the efficacy of its data privacy controls and security measures documented in subsection 2.8.2.
Documented Evidence: • Privacy Policy • Monitoring and Evaluation Report
4.3 Determining new applicable technologies and legal requirements
Objective: A provision in the organization's privacy policy mandating the organization to evaluate any new technologies or new legal requirements that it may affect data processing or data privacy.
Documented Evidence

• Privacy Policy • Risk Assessment • Privacy Impact Assessment

Annex B - Guidelines in Conducting a Privacy Impact Assessment

A Privacy Impact Assessment (PIA) helps both PICs and PIPs navigate the process of understanding the personal data flows within the organization. It identifies various privacy risks, assesses them, and proposes measures to address them.

The identification of risks and the use of a control framework for risk management must consider existing laws, regulations, and issuances relevant to privacy and data protection, as well as the rights of data subjects. The most appropriate standards recognized by the sector or industry of the PIC or PIP, as well as that of the information and communications technology industry, shall also be considered.

The results of a PIA must be properly documented in a report that includes information on stakeholder involvement, proposed measures for privacy risk management, and the processes through which the results of the PIA will be communicated to internal and external stakeholders.

Guidelines	
Preparing for PIA	
Accountability in conducting PIA	Specify the person or unit accountable for managing and assessment of privacy risks.
	Identify process owners, end-users, and relevant stakeholders.
Strategy for conducting PIA	Determine strategies in conducting PIA, its timeline and schedule, etc.
	In determining how the assessment will be done, the organization should decide whether the assessment will be for each determined processes or an accumulation of a unit/division's processes. It will all depend on the organization's requirements and shall consider the conduct of PIA for new processes, programs, and projects within an organization.

Identifying Assets and Requirements	Identify the assets such as processes, projects, systems, or applications that act on personal data that makes it a candidate for PIA.
	Determine the needs in conducting PIA, such as ICT resources, framework, or templates.
Risk Criteria	Define the appropriate risk criteria for the data subjects.
Conducting PIA	
Description	Describe the process, project, system, or application that will be assessed.
	Describe its function and purpose for processing personal data.
Scope	Determine the scale and scope of the assessment in terms of the processes/project/systems/applications, stakeholder, end-user, process owners involved on it.
Stakeholder Engagement	Determine the internal and external stakeholders.
	Determine how stakeholders will be involved in the assessment.
Personal Data Flows	Identify the categories of personal data acted on by the process/system/application/project.
	Describe each data lifecycle of the personal data from collection, usage, storage/retention, disclosure/transfer and disposal/destruction.
Risk Management	Identify the risks relevant to the data subjects, organization, and stakeholders arising from the process/system/project/application.
	List anything else that may impact privacy.
	Describe the adherence of the process/system/project/application to the data privacy principles of transparency, legitimate purpose, and proportionality.
	Describe its adherence to data protection principles of confidentiality, integrity, and availability.
	Identify the possible risks for the data subjects' rights.
	Determine the impact and probability of each identified risk.
	Consider the possible causes and sources of the identified risks and their positive and negative consequences to the data subjects, organization, and stakeholders.

	Evaluate each risk based on the severity of impact on data subjects as well as the overall impact of the organization. A risk map may be used in doing so.
	Choose risk treatments or mitigations to minimize it. Always consider balancing the costs and efforts of implementation against the organization's obligation to the privacy of data subjects and stakeholders.
	Identify the appropriate controls for privacy treatment or mitigation.
	Create privacy risk mitigation plans.
Approval	Seek approval from management regarding the risk mitigation plans.
Continuous Improvement	Determine when to review or conduct another PIA to check the effectiveness and efficiency of risk mitigation plans.

Annex C - Content Requirements – Data Sharing Agreement

A DSA refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties. Only PICs shall be made parties to a data sharing agreement. Where a data sharing agreement involves the actual transfer of personal data or a copy from one party to another, such transfer shall comply with the security requirements imposed by the DPA, its IRR, and all applicable issuances of the NPC.

CONTENT	OBJECTIVE
Purpose(s) and lawful basis	The data sharing agreement shall specify the purpose/s of the data sharing and the appropriate lawful basis.
Objectives	The data sharing agreement shall identify the objective/s that the data sharing is meant to achieve.
Parties	The agreement shall identify all PICs that are party to the DSA and, for each party, specifies the following: - Type of personal data it will share, if any. - Whether the personal data processing will be outsourced, including the types of processing PIPs or service providers will be allowed to perform. - Method to be used for the processing of personal data. - Designated data protection officer.
Term	The agreement shall clearly specify the term or duration of the data sharing agreement which will be based on the continued existence of the purpose/s of such arrangement.
Operational details	The agreement shall contain an overview of the operational details of the data sharing, including the procedure the parties intend to observe in implementing the same. If the recipient will be allowed to disclose the shared data, or grant public access, the following must be established clearly in the DSA: - Justification for allowing such access - Parties that are granted access - Types of personal data that are made accessible - Estimated frequency and volume of such access If disclosure or public access is facilitated by an online platform, the program, middleware, and encryption method that will be used should also be identified.

	Any other information that will sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved shall also be provided.
Security measures	The agreement shall include description(s) of the reasonable and appropriate organizations, physical, and technical security measures that the parties intend to adopt to ensure the protection of the shared data. This includes establishment of a process for data breach management.
Data subject's accessibility	The agreement shall provide mechanisms that allow affected data subjects to exercise their rights relative to their personal data, including: - Identity of the party or parties responsible for addressing information requests, complaints by a data subject, and/or any investigation by the NPC. - Procedure by which a data subject can access or obtain a copy of the DSA. The parties may redact or prevent the disclosure of trade or industrial secrets, confidential and proprietary business information, and any other detail or information that could endanger or compromise their information systems, or expose to harm the confidentiality, integrity, or availability of personal data under their control.
Retention and Data Disposal	The agreement shall include rules for the retention of shared data and identify the method that will be adopted for the secure return, destruction, or disposal of the shared data and the timeline thereof.

Annex D – Objectives, Requirements, Considerations and Guide Questions - Security of Personal Data

The risks identified in the PIA must be addressed by a control framework, which is a comprehensive enumeration of the measures intended to address the risks, including organizational, physical, and technical measures to maintain the availability, integrity, and confidentiality of personal data and to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and contamination (Section 6 of NPC Circular 16-01).

The PIC/PIP must implement reasonable and appropriate organizational, physical, and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other means of unlawful processing.

The determination of the appropriate level of security must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization and complexity of its operations, current data privacy best practices, and the cost of security implementation. The measures implemented must include:

1. Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interface with or hindering of their functioning or availability.
2. A security policy with respect to the processing of personal information.
3. A process for identifying and accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; and
4. Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

a. Physical

1. Perimeter Security

- **Entrance Controls**
  Considerations:

Compliance Objective	Activity	Guide Questions
To verify if the organization has any entry controls for visitors on their facilities that process personal information	Check the following documents and physical controls: 1. Door Locks 2. Security Staffs Duties and Responsibilities 3. Visitor's Logbook 3. Physical security policy	Are there any form locks on doors or physical entries during off-hours or to prevent unauthorized entries or forced entries? Is there a security employee that manages the physical entries of employees and visitors? Is there a policy that sets out the policy and requirements of employee and visitors' requirements upon entrance? Is the date and time of entry and departure recorded by the organization? Are the visitors accessing the facilities supervised, and was their access given prior approval? Is there a logbook or electronic records system that contains the entry and departure of the visitors?

Example:

An organization that has its own office building is currently implementing perimeter security on all of their entrances. Security staff are stationed 24/7 with three (3) shifting schedules and it is always locked during off hours and its key are being held by the designated property administrator of the organization. Security staffs are tasked to assists and make sure to

validate the visitor's purpose of coming inside the organization's facilities. They are only granted access to the specific room and floor that they are needed to.

- **Offices, rooms and facilities**

There should/shall be procedures in minimizing the risks in having access to facilities or production areas where personal data are processed. Employees should be aware of their responsibility in securing areas that contain/handle personal data.

Compliance Objective	Activity	Guide Questions
To verify if the organization has procedures to prevent unauthorized physical access and damage to data processing facilities	Check the following documents and physical controls: 1. Office Key Inventory 2. Clear Desk Policy 3. Access Control Policy	Are the facilities of the organization that process personal data identified? Are the key holders of the facilities being accounted for? Are the outputs such as physical documents, and USB flash drives that contains personal data hidden? Are the employees that process or handle personal data aware of their responsibility in hiding/securing physical documents and USB flash drives that contains personal data?
To verify if the organization restricts the use of	Check the following documents:	Does your organization restrict the use of photographic equipment

photographic media in the production area that process personal data	1. Restricted equipment in the production area	when in the personal data processing area? Are the visitors are not allowed to use their phones and camera equipment upon entering facilities that process personal data?

Example: An organization's office rooms and storage rooms that are used for personal data processing are always locked whenever not in used. Only authorized personnel can only enter the said facilities.

1. Data protection against environmental threats

Compliance Objective	Activity	Guide Questions
To verify if the organization has accounted the physical security against natural disasters or accidents	Check the following document: 1. Business Continuity Plan	Does your organization identify events that may cause operations disruptions? Does your organization have procedures in case natural disasters such as fire, flood, storm etc., affect the workplace or operations? Does your organization have developed procedures to maintain or restore operations and ensure availability should natural events or accidents occur?
To verify if the organization regularly tests its	Check the schedule set up by the management in conducting drills	Does your organization lay out the plans and schedule for testing the

procedures in business continuity	and test plans for business continuity	procedures for business continuity?
To verify if the organization updates its plans and procedures on business continuity based on its test results and risks assessments	Check the privacy impact assessments if there are any recommendations to update the business continuity plan and the gaps or information collected on its test results.	Does your organization find any gaps on its business continuity plan or procedures upon its testing or risk assessment? Does your organization have recommendations to mitigate the gaps found or revisions/updates on its business continuity plans or procedures?

2. Clear Desks

Compliance Objective	Activity	Guide Questions
To verify if the organization has measures to protect personal data being handled or processed by employees (rank and file)	Check the following document: 1. Clear Desk Policy 2. Personal data flows/information classification	Does your organization have procedures for employees (rank and file) to manage physical documents, removable media storage devices and monitors or screens used for personal data processing? Does your organization account for the classification of personal data it processes, and does it communicate its importance to its employees? Are the organization's physical documents that contain personal information and sensitive personal information locked away or hidden except when required access?

To verify if the organization has communicated the responsibility and accountability of the employees that handle or process personal data	Check the following document: 1. Employee Manual 2. Non-Disclosure Agreement	Are the employees aware of their responsibilities in protecting personal data from documents and removable media devices?

3. ICT Asset Management

Compliance Objective	Activity	Guide Questions
To verify if the organization has identified the ICT assets that is used to process personal data	Check the inventory of assets or the record of processing activities if it specifies ICT assets used in personal data processing	Does your organization identify the ICT assets used in processing personal information? Does your organization include the ICT assets to its records of processing activities?
To verify if the organization has defined the appropriate protection measures or responsibilities in protecting the ICT assets used in processing personal data	Check the following document: 1. Asset management policy	Does your organization have an asset management policy that governs the ICT assets used in personal data processing? Does your organization identify employees accountable to the ICT assets? Does your organization's ICT asset management policy specify the responsibilities of the persons in charge of the ICT assets?
To verify if the organization has created and maintained	Check if the organization is currently maintaining an	Does your organization identify the employees accountable to the ICT assets?

documentation to monitor and regulate ICT assets that are used in personal data processing.	inventory of assets and its employees in charge on it	Does your organization regularly update its inventory of ICT assets? Does your organization classify the ICT assets that are used to process sensitive personal information?

Example: An organization has identified possible risks that their office may encounter through natural threats and implemented a business continuity plan. A couple of months have passed, and a fire incident occurred near their building that could potentially affect their data center. Fortunately, it is one of the risks that they have identified and part of their business continuity plan. They first alerted their employees to evacuate before it reaches the building. The fire eventually reached the building ultimately destroying the data center. But with their effective business continuity plan, combined with a resilient data infrastructure, the organization was able to full restore their service withing a few hours.

4. Mobile Device Equipment

Compliance Objective	Activity	Guide Questions
To verify if the organization has secured the usage of mobile devices	Check the following documents: 1. Mobile device policy	Does your organization account the risks brought in by the using mobile devices in areas/facilities that process personal data? Does your organization register or maintain an inventory of mobile devices issued by the organization to its employees? Does your organization specify physical protection for the use of mobile devices?

		Does your organization restrict installation of software applications that are outside its white-listed applications? Does your organization require software installation and security patches to its mobile devices? Does your organization implement encryption or cryptographic techniques to add security layer on the organization-issued mobile devices? Does your organization implement measures for malware protection on mobile devices? Does your organization implement measures for remote wiping or disabling in the event of loss of mobile devices? Does your organization implement backup procedures for its mobile devices?

Example:

An organization that issues office laptops have set out requirements to the devices and employees before of its deployment. All mobile devices are registered as well as the employees accountable for it. There

is also a restriction of software to be installed, only applications that are advised by the MIS unit are only allowed.

5. Disposal or re-use of ICT assets

Compliance Objective	Activity	Guide Questions
To verify if the organization has securely disposed ICT assets when no longer used	Check if the organization has procedures for disposing ICT assets that were used in processing personal data	Does your organization identify the ICT assets that will be requiring secure disposal? Does your organization identify a threshold for ICT assets that can still be re-used? Does your organization identify and establish secure and proper disposal of hard drive and external hard that contains personal data? Does your organization have an inventory of ICT assets that were disposed?

Example: The property custodian of an organization sets a retention period on their ICT resources. When the equipment reached its termination period, they assess it and categorize if it can still be used or for disposal. If the its for disposal, ICT employees remove the hard drives for properly disposal.

b. Technical

1. User access management

Compliance Objective	Activity	Guide Questions
To verify if the organization has established procedures or measures in managing user access on its process, systems and software applications	Check if the organization has a registration and de-registration process for its systems and processes	Does your organization designate or unique user id/username for each employee who will be accessing the organization's systems, processes and applications? Does your organization disable or remove users who are separated from the organization?
To verify if the organization ensures that only authorized user can only access personal data	Check if the organization has established rules and policies for registered users to only access what is authorized	Does your organization have a documented process flow of authorizing employees to allow access on its systems or applications?
To verify if the organization has procedures to prevent unauthorized access to process, systems, and applications	Check if the organization has procedures to mitigate unauthorized access to process, systems and applications within its domain.	Does your organization record the authorization of employees from the process owners of the systems or application?

Example: An organization has a set of process of authoring employees or new employees to have access or use their systems and applications. This process will be used to manage throughout the lifecycle from identification of a user to the granting, modification and revocation of a user's access privilege.

2. Encryption

Compliance Objective	Activity	Guide Questions
To verify if the organization has used encryption methods to protect the confidentiality and integrity of personal data	Check if the organization has an encryption policy to protect personal data especially sensitive personal information and confidential information	Does your organization identify the strength and type of encryption that will be used? Does your organization implement encryption measures on personal data in transit, at rest and in use? Does your organization use encryption measures to protect personal data transferred through mobile devices or removable media devices or communication line? Does your organization implement a key management system? Does your organization assign or designate a person or group of persons for the implementation of encryption measures or procedures? Does your organization implement a secure socket layer (SSL) or transport layer security for website? Does your organization implement encryption methods to protect its email?

Example:

An organization that provides services online has it hosted on a web application. This web application can be found at their website. Users can avail the service through registering an account by filling out the online forms with their personal information. To protect the transaction as well as the personal information of the user, the organization have implemented a security measure of encrypting the data in transit and at rest that are being processed by the web application.

3. Authentication and Authorization

Compliance Objective	Activity	Guide Questions
To verify if the organization provides authentication process for employees before accessing personal data through credentials	Check if the organization has user registration process for its application and software	Does your organization have a user registration process to facilitate assignment of access rights for its systems, application and software? Does your organization assign unique user ids for each employee who will be accessing their system, application or software? Does your organization ensure that redundant user ids are not allowed?
To verify if the organization has taken measures to prevent unauthorized access to its systems and applications	Check if the organization has the following documents: 1. List of user ids and their privileges 2. Record of employees' access rights 3. Periodic review of the access rights. 4. Procedure for removal of user ids and access rights	Does your organization verify the level of access granted and privileges to each employee is appropriate? Does your organization have a process for assigning and approving/revoking the access rights granted to employees? Does your organization have list of all the user ids, its owners and its privileges?

		Does your organization regularly review the employees and their privileges? Does your organization immediately remove or revoke user ids and their privileges of employees who left the organization?
To verify if the organization has established procedures in authorizing employees in processing personal data	Check if the organization has authorization of access rights or privileges	Does your organization have authorization process for granting access rights and privileges from its process owner/management?

Example: An organization has implemented a digital repository that is accessible through an implementation of intranet. This repository will hold the confidential documents and information that should only be viewed only by certain employees of certain divisions. An internal policy was implemented alongside with an access control within the repository system to limit and restrict the access to specific group of employees.

4. Password management

Compliance Objective	Activity	Guide Questions
To verify if the organization has deployed a credential process to authenticate employees that are accessing personal data	Check if the organization has a password management policy	Does your organization require individuals who are maintaining credentials (user id and password) to ensure accountability when processing personal data? Does your organization impose a choice of quality of passwords?

		Does your organization enforce employees the regular updating of employee passwords? Does your organization prohibit re-using of old passwords? Does your organization implement ways to redact passwords on the monitor when being entered?

Example: The organization implements a credential authentication to have access to their systems such as emails, and online repositories. The authentication is based on an identifier or username and a password. They have implemented a policy to set a minim number of combination of characters of the employees' password. They also set a systematic renewal of password update to further limit the chance of compromise.

5. Capacity management

Compliance Objective	Activity	Guide Questions
To verify if the organization has established procedures providing employees the capacity to manage assets and resources used in personal data processing	Check if the organization has activities or procedures to enable employees that process personal data	Does your organization conduct trainings to employees who will process personal data through different ICT resources? Does your organization provide sufficient employees knowledge employees in the deletion of obsolete data whenever no longer needed?

		Does your organization provide sufficient capacity in decommissioning applications, systems, and databases? Does your organization provide sufficient capacity in optimizing applications and its logics or functions? Does your organization provide sufficient capacity restricting bandwidth for resource-driven services? (e.g., video streaming, video rendering, etc.,)

Example: An organization has established their privacy management program and implemented it through their privacy manual to help ensure data protection for their organization. One of their programs is to have a periodic security awareness training to develop essential competencies on new techniques and methods that are essential in facing possible security issues. The awareness programs provide ways to educate the employees and to motivate them to take data privacy and data protection seriously and respond accordingly.

6. Digital data management

Compliance Objective	Activity	Guide Questions
To verify if the organization properly manages the digital data it handles/controls	Check if the organization's information classification inventory includes digital media.	Does your organization include digital data on its inventory of information? Does your organization identify whether there are digital data that fall under personal information,

		sensitive personal information and privilege information?
To verify if the organization has established the lifecycle of the digital data, it handles	Check if the organization has a document that explicitly explains the lifecycle of digital data from its collection, usage, storage and retention, sharing and disposal	Does your organization have a lifecycle documentation that discusses stages of collection, usage, storage and retention, sharing up to disposal? Does your organization identify the employees in charge for each stage?

Example: As an organization transition its manual process to automated, it started to list all information, especially the personal data that its automated process will be dealing with. Before the transition, they already have an inventory on information that was being processed physically which also helps them to further identify the digital data. Having the inventory for their personal information assets was able to improve the organization's vision of data lifecycle digitally and anticipate the possible harm that might occur on each stage,

7. Data masking/redaction of digital and physical documents

Compliance Objective	Activity	Guide Questions
To verify if the organization utilizes a process of masking/redacting personal data on digital documents that will be shared externally	Check if the organization has procedures on masking/redaction of personal data that will be shared to another party	Does your organization have masking/redaction procedures for digital data that contains personal data? Does your organization have masking/redaction procedures for physical files (e.g., documents, forms, etc.,) that contains personal data? Does your organization have masking/redaction procedures for

		documents that will be reproduced?

Example: An organization implements a redaction procedure for their documents before they share or disclose it publicly. They redact the personal information that are not necessary to be disclosed to the public. The document is still valuable to its purpose which is to give reference on the situations, use cases and reference to their queries but at the same time it protects that privacy of the individuals that are in the document.

8. Data leakage prevention

Compliance Objective	Activity	Guide Questions
To verify if the organization has procedures against data leakage on their systems and applications	Check if the organization has incorporated their access control policy to prevent data leakage that will be caused by employees.	Does your organization establish measures to prevent data leakage on its access control policy? Does your organization implement sanctions against employees who commits leakage of personal data? Does your employees have knowledge of their responsibility and accountability on the personal data they process?

Example: Security measures such as closely monitoring the network for unwanted or malicious emails that may contain malware or confidential documents or information that are disclose to an unauthorized person, are implemented to prevent data leakage.

9. Monitoring control/activities/logging

Compliance Objective	Activity	Guide Questions
To verify if the organization has procedures and controls to monitor activities and logs.	Check if the organization has incorporated its access control and acceptable use policies to monitor activities and logs.	Does your organization establish measures to monitor activities and logs as indicated in its access control and acceptable use policies? Does your organization implement sanctions against employees who commit unauthorized or malicious activities? employees

Example:
To ensure that employees activities are conformance of the organization's policy, they have established a monitoring system that supervise the employees' activities legitimate to its purpose. This enables them to prevent malicious activities that could lead to data leakage or unauthorized disclosure of personal data.

10. Software management

Compliance Objective	Activity	Guide Questions
To verify if the organization has procedures on ensuring the integrity of operational software systems	Check if the organization has the following documents: 1. Conformance Policy for Software Acquisition/Procurement 2. Software Installation Policy 3. Software Vulnerability Assessment Policy 4. Privacy Impact Assessment of Software Applications	Does your organization have a conformance checking procedures to validate software applications or systems for acquisition/procurement? Does your organization have extensive procedures that cover its usability and security before acquisition and installation/deployment?

		Does your organization certify/approve software application before its installation/deployment? Does your organization only allowed certified or approved software application to be installed? Does your organization conduct tests to see if there are vulnerabilities on the software applications/systems? Does your organization document and consider all the vulnerabilities found in the vulnerability tests? Does your organization conduct privacy impact assessments before its deployment?
To verify if the organization regularly evaluates vulnerabilities of their deployed software and measures are implemented to mitigate it	Check if the organization has documents and reports the vulnerabilities found on assessments	Does your organization establish and define employees who are responsible with the technical vulnerability management and monitoring, assessment, tracking and patching? Does your organization maintain its awareness on the technical vulnerabilities and its possible implications? Does your organization have a timeline in addressing the technical vulnerabilities?

		Does your organization have tested the possible or identified patch for the technical vulnerability before implementing them? Does your organization maintain an audit log for the procedures taken to mitigate the technical vulnerabilities?

Example: As an organization conducts their PIA, they have come to an observation that their software applications are quite essential to their day to day activities. The applications are combination of subscription, one-time purchases and developed. Upon reviewing many divisions are looking to further procure more applications for the coming years. In order to manage all of their software applications, they have minimum requirements for software applications that they will procure or develop. This procedure analyzes the application if it eligible to use by the organization. It helps to minimize the risk of having vulnerable software.

11. Network security

Compliance Objective	Activity	Guide Questions
To verify if the organization has data protection in networks and its other supporting information facilities	Check if the organization manages and controls its network infrastructure, facilities, systems and applications	Does your organization establish and define the employees responsible for network security? Does your organization have procedures to safeguard the confidentiality and integrity of data communicated over public networks? Does your organization have procedures to safeguard connected

		systems and applications to the network? Does your organization enable the monitoring, recording and detection of actions that can affect the operations? Does your organization authenticate its network activities? Does your organization restrict its system connections appropriately?

12. Security incident reporting

Compliance Objective	Activity	Guide Questions
To verify if the organization responds accordingly to the security incidents in accordance with the documented procedures	Check if the organization has the following documents: 1. Formulation of Data Breach Response Team 2. Security Incident Management Policy 3. List of Incident Response Procedures 4. List of contacts of authorities 5. Annual Security Report(s)	Does your organization identify and designate a team that will handle the possible data breach? Does your organization identify the required procedures for security incident management? Does your organization integrate the risks identified on the PIAs to feed into its security incident management policy(s)? Does your organization have a list of pre-defined procedures if a classified breached or incident occurred?

		Does your organization identify appropriate and updated contacts of regulatory authorities (i.e., NPC, NBI, PNP – Cybercrime etc.,) Does your organization have a records of annual security incidents and attempts?
To verify if the organization collects substantial data and evidence for the purposes of legal and disciplinary action	Check if the organization documented evidence collected from the breaches or incident that occurred	Does your organization establish procedures in gathering data from previous security incident and data breaches that occurred? Does your organization maintain document(s) to that contains the data from previous security incidents and data breaches?
To verify if the organization established procedures in reporting security incidents and breaches to NPC or any other authorities	Check if the organization have procedures in communicating with the authorities when a security incident or data breach does occur?	Does your organization have the contact information of authorities (i.e., NPC, NBI, PNP, etc.,)? Does your organization have approved protocols to communicate with the authorities in the event of a security incident and data breach?

Example:

An organization has been victimized by a hacker which resulted to a website defacement which rendered their online services inaccessible for a couple of hours. Months before the incident they have already established a data breach response team that would be responsible for these cases. The organization immediately activates the team and looms an investigation of the issue and they initiated procedures to mitigate and restore its online services. A few hours later they were able to restore and renew the credentials of their online services. The investigation had led to discover the culprit of the defacement and the vulnerability of their website.

13. Cloud management

Compliance Objective	Activity	Guide Questions
To verify if the organization that uses cloud services have controls for personal data protection	Check the following documents: 1. Outsourcing contract with the cloud provider 2. Cloud Accountability Model/Chart 3. Access Control Policy for Cloud Services 4. Cloud provider Certification 5. Backup Policy	Does your organization specify the importance of the personal data protection embedded in the outsourcing contract? Does your organization's outsourcing contract with the cloud provider clear the responsibilities of the parties to ensure data protection? Does your organization have a chart or equivalent documentation that states the responsible persons that has administrative rights in cloud infrastructure management? Does your organization have an access control policy for its employees accessing their cloud services? Does your organization monitor its employees' access and activities on its cloud services? Does your organization require their cloud provider to be certified for ISO/IEC 27018? Does your organization backup its data on its cloud?

Example: An organization that employs cloud services on public cloud platform has established a monitoring of its assets that are in them. This helps them keep track of their personal information assets and any other services that are in the cloud.

14. Security Clearance

Legal Basis: 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 source organization. (Section 23.a of the DPA of 2012)

A source organization shall strictly regulate access to sensitive personal information under its custody or control, particularly when it allows online access. An employee of the government shall only be granted a security clearance when the performance of his or her official functions or the provision of a public service directly depends on and cannot otherwise be performed unless access to the personal data is allowed.

Considerations:

Compliance Objective	Activity	Guide Questions
To verify if the organization has classified the sensitive personal information it handles	Check the following documents: 1. Personal Data Inventory 2. Records of processing activities	Does your organization identify the divisions and offices that process sensitive personal information? Does your organization identify the process owners and risk owners who process sensitive personal information? Does it reflect to the personal data inventory or records of processing activities?
To verify if the organization has controls to govern the access and processing of sensitive personal	Check the following documents:	Does your organization limit access to sensitive personal information it

information to authorized employees only	1. Access Control Policy	handles by restricting it to authorized employees only? Are the authorized employees aware of their responsibility to protect the sensitive personal information they process?
To verify if the organization implements security clearance policy when employees ask for access to sensitive personal information	Check the following document: 1. Security Clearance Policy/Process 2. Personal Information Access Request Form	Does your organization have a process in approving employees or other divisions/offices that request access for sensitive personal information for valid purposes? Is the request being documented through an application form or request form signed by the head of the organization? Does the head of the organization approve the security clearance for these requests?

15. Telecommuting

Legal Basis: The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing (Section 20.a of the DPA of 2012)

An organization shall consider alternate working arrangements in any given public health emergency situations that would require telecommuting workforce strategy to balance health and safety with the organization's need to continuously operate and provide essential services.

Considerations:

Compliance Objective	Activity	Guide Questions

To verify if the organization ensures that all of its ICT assets and equipment are secured and shall only be used to perform the organizational-related tasks and only by its authorized employees.	Check the following: 1. Authorized ICT Assets Inventory	Does your organizations have an inventory of ICT assets and labeled which were deployed for telecommuting? Does the inventory contain the employees assigned to each ICT asset for telecommuting? Does all the ICT assets deployed for telecommuting have been cleared and provided with the necessary tools/applications to perform the authorized tasks?
To verify if the organization grants its employees the privilege of using personally owned devices if it is documented and approved by their immediate supervisor.	Check the following: 1. Bring-Your-Own-Devices (BYOD) Policy 2. BYOD Clearances	Does the organization has a policy or policies to allow BYOD to perform the organization's tasks and services? Does the organization has established a clearance mechanism to allow the use of BYOD?
To verify if the organization ensures that it implements an Acceptable Use Policy that covers the telecommuting procedures	Check the following 1. Telecommuting policy 2. Acceptable use policy	Does your organization provide additional guidance on its acceptable use policy that covers telecommuting? Does it cover additional procedures on accessing different type of services,

		such as websites and application?
To verify if the employees' access to data and assets and equipment is at the lowest level as possible	Check the following: 1. Access Control Policy	Does the organization cover the telecommuting policy on its access control policy? Does the organization's policy determine the rights, privileges and permissions given to the telecommuting employees?
To verify is the organization implements procedures and policy for authorizing and authenticating its employees.	Check the following: 1. Authorization policy and procedures 2. Authentication policy and procedures	Does the organization established authenticating procedures for employees accessing its assets and services that are part of the telecommuting workforce? Does the organization established authorization procedures for employees accessing its assets and services that are part of the telecommuting workforce? Does the organization implements procedures to define and review the roles, privileges and permissions given to the authorized employees?
To verify if the organization has ensured the protection of personal data inside their network or communicate withing its network by implementing controls that shall manage the information coming from different outlets	Check the following: 1. Network security policy 2. Email policy 3. Communications policy	Does the organization have setup controls to manage incoming and outgoing information from its network? Does the policy include standards in submitting

of the the telecommuting protocols		facets of data within the organization network infrastructure? Does the organization has set up its official communication outlet for those employees in telecommute?
To verify if the organization have incorporated its readiness in telecommuting within the security incident and personal data breach management	Check the following: 1. Personal data Breach Management Policy 2. Telecommuting policy	Does the security incident and data breach management policies include reporting of security events or potential security events in telecommute? Does it provide the procedures on how to contact the authorized personnel when there is a security event or potential security event during the implementation of telecommute strategy?