Republic of the Philippines
NATIONAL PRIVACY COMMISSION

**NPC Circular Year-NO.**

**DATE : XX Month XXXX**

**SUBJECT : SECURITY OF PERSONAL DATA IN PUBLIC AND PRIVATE SECTORS**

**WHEREAS**, Article II, Section 24 of the 1987 Constitution provides that the State recognizes the vital role of communication and information in nation-building. At the same time, Article II, Section 11 thereof emphasizes that the State values the dignity of every human person and guarantees full respect for human rights;

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

**WHEREAS**, pursuant to Chapter II, Section 7 of the abovementioned statute, the National Privacy Commission is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by personal information controllers with the provisions of the Act and with international standards 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**, under Rule III, Section 9 of the *Implementing Rules and Regulations* (IRR) of the Data Privacy Act of 2012 provides that the Commission's functions, among others, are to develop, promulgate, review or amend rules and regulations for the effective implementation of the Act;

**WHEREAS**, pursuant to Chapter V, Section 20 of the same law, the personal information controller must implement reasonable and appropriate *organizational*, *physical* and *technical* measures intended for the protection of personal information;

**WHEREAS,** under Chapter VII, Section 22 of the same law, the head of each government agency or instrumentality is responsible for complying with the security requirements mentioned in the law. This includes ensuring all sensitive personal information maintained by his or her agency are secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission;





5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

**WHEREAS**, under Section 23 of the same law, the Commission may issue guidelines relating to access by agency personnel to sensitive personal information;

**WHEREFORE**, the abovementioned premises considered, the National Privacy Commission hereby issues this Circular governing the security of personal data in government agencies and the private sector.

## RULE I.
## GENERAL PROVISIONS

**SECTION 1.** ***Scope.*** **-** This Circular shall apply to all natural or juridical persons engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the Data Privacy Act, its Implementing Rules and Regulations, and other relevant issuances of the National Privacy Commission.

**SECTION 2.** ***Purpose.*** **-** This Circular aims to provide updated requirements for the security of personal data in government agencies and the private sector, due to the ever-changing security threat and technology landscape.

**SECTION 3.** ***Definition of Terms***. **-** For the purpose of this Circular, the following terms are defined as follows:

A. "*Business Continuity*" refers to the capability of a Personal Information Controller/s or Processor/s to continue the delivery of products or services at acceptable pre-defined levels following disruptive events;
B. "*Business Continuity Plan*" refers to documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruptive events;
C. "*Disruptive Events*" refers to any occurrence or change that interrupt planned activities, operations, or functions, whether anticipated or unanticipated;
D. "*Encryption*" refers to the reversible transformation of data by a cryptographic algorithm to produce ciphertext so as to hide the information content of the data;
E. "*Privacy-by-Design*" is an approach to the development and implementation of projects, programs, and processes that integrates into the design or structure safeguards that are necessary to protect and promote privacy, such as appropriate organizational, technical, and policy measures;
F. "*Privacy-by-Default*" is the principle according to which an organization (the personal information controller) ensures that only data necessary for each specific purpose of the processing are processed by default (without the intervention of the user or the data subject);
G. "*Private Entity*" refers to any natural or juridical person, or any other body that is not a unit of the Philippine government or any other foreign government entities, such as but not limited to, stock and non-stock corporations, foreign corporations, partnerships, cooperatives, sole proprietorships, or any other legal entity.

**SECTION 4.** ***General Obligations.*** **-** A PIC shall observe the following duties and responsibilities, in addition to its obligations under the DPA:





5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

A. Designate and register its Data Protection Officer (DPO) with the Commission, taking into account the provisions of the (DPA), its (IRR), its amendments or any other issuance of the Commission pertaining to the designation and registration of DPOs;
B. Create an inventory of all the data processing systems and activities, taking into account Section 20(c) of the IRR;
C. Register its data processing systems with the Commission according to the provisions of the DPA, its IRR, its amendments, or any other issuance of the Commission pertaining to the registration of data processing systems;
D. Conduct a Privacy Impact Assessment for each program, process, or measure that involves processing of personal data: Provided, that such assessment shall be updated as necessary. Likewise, controls which were previously assessed and implemented shall be monitored, evaluated, and incorporated into a Privacy Management Program of a PIC;
E. Create privacy and data protection policies to set and standardize the governance of the processing of personal data, taking into account the privacy impact assessments, as well as Sections 25 to 29 of the IRR;
F. Implement data protection measures such as organizational, physical, and technical security measures, taking into account sections 25 to 29 of the IRR;
G. Conduct PIC and PIP-wide training on privacy and data protection policies at least once a year: Provided, that a similar training shall be conducted during all orientations for newly hired or contracted personnel by the PIC; and
H. Comply with the Commission's order when the PIC's privacy and data protection policies are subject for review and assessment, in terms of their compliance with the requirements of the DPA, its IRR, and all issuances by the Commission.

**SECTION 5.** ***Control Framework for Data Protection***. **-** The risks identified in the Privacy Impact Assessment must be addressed by a control framework. The contents of a control framework shall take into account, among others, the following:

A. Nature of the personal data to be protected;
B. Risks represented by the processing, the size of the organization, and the complexity of its operations;
C. Current data privacy best practices; and
D. Cost of security implementation.

**SECTION 6**. ***Privacy Impact Assessment.*** **-** A PIC shall ensure that its conduct of a Privacy Impact Assessment is proportionate and consistent with the amount and sensitivity of the personal data being processed, and the adverse risks which may arise from the unauthorized processing of personal data.

The Privacy Impact Assessment shall include the following:

A. a data inventory identifying:

   i. the types of personal data held by the PIC, including records of its own employees;
   ii. list of all information repositories holding personal data, including their location;
   iii. types of media used for storing the personal data and risks associated with the processing of the personal data;


5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

B. a systematic description of the processing operations anticipated and the purposes of the processing, including the lawful criteria pursued by the PIC;

C. an assessment of the necessity and proportionality of the processing in relation to the purposes of the processing; and

D. an assessment of the risks to the rights and freedoms of a data subject.

## RULE II.
## EMBEDDING PRIVACY-BY-DESIGN

**SECTION 7.** ***Privacy-By-Design and Privacy-By-Default.*** **-** A PIC shall ensure that the requirements stated in this Circular and the general data privacy principles (*Legitimate Purpose*, *Transparency* & *Proportionality*) shall be implemented during the planning phase of its data processing systems for the integration of data protection into these systems. The identified data protection requirements shall then be implemented by default into any personal data processing without any action from the data subject.

The PIC shall conduct a Privacy Impact Assessment for their off-the shelf software, solutions or data processing systems following the requirements in Section 6 of this Circular. The PIC shall ensure that any functions that do not have legal bases for processing or are incompatible with the specific, declared and intended purposes of processing are switched 'off'.

**SECTION 8.** ***Privacy Engineering.*** **-** A PIC shall adopt the privacy-by-design principles in developing, implementing, and deploying systems, processes, software applications, and services throughout the processing of personal data.

**SECTION 9.** ***Automated Processing.*** **-** A PIC that develops or implements a software application that carries out any automated processing operations shall embed privacy-by-design and privacy-by-default principles by separating its components and applying data protection measures throughout the processing.

The data subject has the right to be informed especially when automated processing becomes the sole basis for making decisions about them and when such decisions would significantly affect them. The software application shall be documented, and the PIC shall notify the Commission and data subjects upon registration of the data processing system with the Commission, and on such other instances as may be required by the Commission. Such notification shall follow the requirements in Section 8 of this Circular and provide the following information:

i. Methods and logic utilized for automated processing; and
ii. Decisions relating to the data subjects that would be made based on processed data or that would significantly affect the rights and freedoms of the data subjects.

## RULE III.
## STORAGE OF PERSONAL DATA

**SECTION 10.** ***General Rule.*** **-** Personal data being processed by a PIC shall be stored in a data center, which may or may not be owned and controlled by such PIC: *Provided*, that the PIC must be able to demonstrate to the Commission how its control framework for data protection, and, where applicable, that of its service provider, shall ensure compliance with the Act: *Provided further*, that where a service provider is engaged, the Commission may require the PIC to submit its contract with its service provider.

**SECTION 11.** ***Encryption of Personal Data.*** **-** All personal data that are digitally processed must be adequately protected, whether at rest or in transit.

Passwords or passphrases used to access personal data should be of sufficient strength (i.e., length, character casing, inclusion of numbers and special characters, do not contain any personal information) to deter password attacks. Each PIC should issue and enforce a Password Policy. The policy shall outline the guidelines for password complexity requirements, periodic password resets, and password best practices.

**SECTION 12.** ***Restricted Access.*** **-** A PIC is required to implement an Access Control Policy. Access to all data centers owned and controlled by a PIC shall be restricted to PIC or its PIP personnel that have the appropriate security clearance. This should be enforced by an access control system that records when, where, and by whom the data centers are accessed. Access records and procedures shall be reviewed by PIC or PIP management regularly.

**SECTION 13.** ***Service Provider as Personal Information Processor.*** **-** When a PIC engages a service provider for the purpose of storing personal data under the PIC's control or custody, the service provider acts as a PIP. It is the responsibility of the PIC to ensure that its PIP has implemented appropriate security measures for the protection of personal data and is able to demonstrate compliance with all the requirements of the DPA, its IRR, and all applicable issuances by the Commission. The obligation to comply with all the requirements of the DPA, its IRR, and all applicable issuances by the Commission with regard to the particular data processing system shall remain with the PIC.

**SECTION 14.** ***Audit.*** **-** The Commission reserves the right to audit, a PIC's data center, or, where applicable, that of its service provider.

Independent verification or certification by a reputable third party may also be accepted by the Commission.

**SECTION 15.** ***Archives.*** **-** The requirements of this Circular shall also apply to private[1] and public archives[2].

## RULE IV.
## ACCESS TO PERSONAL DATA

**SECTION 16.** ***Access to or Modification of Databases.*** **-** Only programs licensed to or owned by a (PIC) shall be allowed to access and modify databases containing the personal data under the control or custody of that PIC.

[1] "Private archives" refers to records belonging to private individuals and/or entities which are of enduring archives value.
[2] "Public archives" refers to public records that are under the custody and control of the National Archives of the Philippines executive director.



5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

**SECTION 17.** ***Security Clearance.*** **-** A PIC shall strictly regulate access to personal data under its control or custody. It shall grant access to personnel, through the issuance of a security clearance by the PIC/PIP head, only when the performance of official functions or the provision of a public service directly depends on such access or cannot otherwise be performed without such access.

A copy of each security clearance must be filed with the PIC's Data Protection Officer.

**SECTION 18**. ***Contractors, Consultants, and Service Providers.*** **-** Access to personal data by independent contractors, consultants, and service providers engaged by a PIC shall be governed by strict procedures contained in formal contracts, which provisions must comply with the DPA, its IRR, and all applicable issuances by the Commission. The terms of the contract and undertakings given shall be considered by the Commission in evaluating the security measures implemented by the PIC.

**SECTION 19.** ***Acceptable Use Policy.*** **-** A PIC shall have an up-to-date Acceptable Use Policy regarding the use by PIC personnel of information and communications technology. The policy shall be explained by the PIC to all personnel who shall use such technology in relation to their functions. Each user shall agree to such policy and, for this purpose, sign the appropriate agreement or document, before being allowed access to and use of the technology.

**SECTION 20.** ***Online Access to Personal Data.*** **-** PIC personnel who access personal data online shall authenticate their identity via a secure encrypted link and must use multi-factor authentication. Their access rights must be defined and controlled by a system management tool.

**SECTION 21.** ***Local Copies of Personal Data Accessed Online.*** **-** A PIC shall adopt and utilize technologies that prevent personal data accessible online to authorized personnel from being copied to a local machine or the computer that a user is currently using on a computer network. The PIC shall also provide for the automatic deletion of temporary files that may be stored on a local machine by its operating system.

Where possible, PIC personnel shall not be allowed to save files to a local machine. They shall be directed to only save files to their allocated network drive.

Drives and USB ports on local machines may also be disabled as a security measure. A PIC may also consider prohibiting the use of cameras in areas where personal data is displayed or processed.

**SECTION 22.** ***Authorized Devices.*** **-** A PIC shall ensure that only known devices, and properly configured to the PIC's or PIP's security standards, are authorized to access personal data. The PIC shall also establish solutions, which only allow authorized media to be used on its computer equipment.

**SECTION 23.** ***Remote Disconnection or Deletion.*** **-** A PIC shall adopt and use technologies that allow the remote disconnection of a mobile device owned by the PIC, or the deletion of personal data contained therein, in the event such mobile device is lost. A notification system for such loss must also be established.

**SECTION 24.** ***Physical Filing System.*** **-** If personal data is stored in any physical media, such as paper-based filing system, a PIC shall maintain a log, from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall also indicate whether copies of the file were made. The PIC management shall regularly review the log records, including all applicable procedures.

**SECTION 25.** ***Personal Data Sharing Agreements***. **-** Access by other parties to personal data under the control or custody of a PIC shall be governed by the Commission's Circular on Data Sharing Agreements.

## RULE V.
## BUSINESS CONTINUITY

**SECTION 26.** ***Telecommuting***. **-** The Commission supports the adoption of a telecommuting or alternative work arrangements as a viable strategy to balance the health and safety of a PIC's or PIP's workforce with its need to continuously operate and provide essential products and services.

A PIC shall define, implement, and communicate its telecommuting policy to its personnel to equip and prepare them.

**SECTION 27.** ***Business Continuity Management.*** **-** A PIC must have a Business Continuity Plan to mitigate potential operational disruptions due to unforeseen events. It must consider the following:

i. Personal data backup, restoration and remedial time;
ii. Periodic review and testing of the business continuity plan which takes into account disaster recovery, privacy/business impact analysis, and crisis communications plan, among others; and
iii. Contact information and other business-critical matters, i.e., electrical supply, building facilities, IT assets, etc.

**SECTION 28.** ***Emails.*** **-** A PIC that transfers personal data by email must either ensure that the data is adequately protected or use secure transmission and reception of email messages, including their attachments. Passwords should be sent through different means. It is also required that agencies utilize systems that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if appropriate, prevent its transmission.

**SECTION 29.** ***Personal Productivity Software.*** **-** A PIC shall implement access controls to prevent themselves and its PIP's personnel from printing or copying personal data to personal productivity software like word processors and spreadsheets that do not have any security or access controls in place.

**SECTION 30.** ***Removable Optical Media.*** **-** A PIC that uses optical media such as compact discs, digital versatile discs, and USB flash drives for processing personal data, shall not be allowed: *Provided*, that if such mode of transfer is unavoidable or necessary, then encryption shall be implemented.





5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

**SECTION 31.** ***Fax Machines.*** **-** Facsimile technology shall not be used for transmitting documents containing personal data.

**SECTION 32.** ***Transmittal.*** **-** A PIC and its PIP that transmit documents or media containing personal data by mail or post shall make use of registered mail or, where appropriate, guaranteed parcel post services and Private Express and/or Messengerial Delivery Service (PEMEDES). It shall establish procedures that ensure that such documents or media are delivered only to the person to whom they are addressed, or his or her authorized representative: *Provided*, that similar safeguards shall be adopted relative to documents or media transmitted between offices or personnel of the PIC and its PIPs.

## RULE VI.
## GUIDELINES FOR DISPOSAL OF PERSONAL DATA

**SECTION 33.** ***Deletion of Personal Data***. **-** In establishing policies and procedures for disposal of personal data, a PIC shall take into consideration the following:

i. Set retention period of data;
ii. Jurisdiction-specific laws, regulations, and existing contracts;
iii. Identify relevant de-identification, anonymization, or deletion techniques for specific types of data;
iv. Required documentation before the deletion, de-identification, or anonymization of personal information.

**SECTION 34.** ***Procedures for Disposal.*** **-** Procedures must be established regarding the secure manner of disposing personal data that would render further processing impossible:

i. Proper disposal of files that contain personal data, whether such files are stored on paper, film, optical or magnetic media;
ii. Secure disposal of computer equipment, such as disk servers, desktop computers, and mobile phones at end-of-life, especially storage media: Provided, that the procedure shall include the use of degaussers, erasers, and physical destruction devices; and
iii. Proper disposal of personal data stored offsite.

**SECTION 35.** ***Third-Party Service Providers.*** **-** A PIC may engage a service provider to carry out the disposal of personal data under its control or custody: Provided, that the service provider shall contractually agree to the PIC's or PIP's data protection procedures and ensure that the confidentiality of all personal data is protected.

## RULE VII.
## MISCELLANEOUS PROVISIONS

**SECTION 36.** ***Personal Data Breach Management.*** **-** In case of a personal data breach or security incident, a PIC shall comply with the requirements of the Commission's Circular on breach management.





5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228

**SECTION 37.** ***Penalties***. **-** Violations of these Rules, shall, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent ban on the processing of personal data, or payment of fines, in accordance with the DPA, its IRR, and the Commission's issuances.

Failure to comply with the provisions of this Circular can result in criminal, civil, administrative liabilities, and disciplinary sanctions against any erring officer or employee in accordance with existing laws or regulations.

The commencement of any action under this Circular is independent and without prejudice to the filing of any action with the regular courts or other quasi-judicial bodies.

**SECTION 38.** ***Amendments***. **-** These Rules shall be subject to regular review by the Commission. Any amendment thereto shall be subject to the necessary consultations with the concerned stakeholders.

**SECTION 39. -** ***Transitory Period***. **-** A PIC shall be given a transitory period of eighteen (18) months from the effectivity of these Rules to comply with the requirements of this Circular.

**SECTION 40.** ***Separability Clause***. **-** If any portion or provision of these Rules is declared null and void or unconstitutional, then the other provisions not affected thereby shall continue to be in force and effect.

**SECTION 41.** ***Repealing Clause***. **-** This Circular expressly repeals the Commission's Circular No. 16-01. The provisions of the IRR and all other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified.

**SECTION 42.** ***Effectivity***. **-** These Rules shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

**JOHN HENRY D. NAGA**
Privacy Commissioner

**LEANDRO ANGELO Y. AGUIRRE**
Deputy Privacy Commissioner





5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph Tel No. 8234-2228