NPC Circular 2023-06

Date : 01 December 2023

Subject : Security of Personal Data in the Government and the Private Sector

WHEREAS, Section 2 of Republic Act No. 10173, otherwise 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 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 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 ensuring the compliance of personal information controllers (PICs) 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 data in the country, in coordination with other government agencies and the private sector;

WHEREAS, Rule III, Section 9 of the *Implementing Rules and Regulations* of the Data Privacy Act of 2012 (IRR) provides that the NPC's functions, among others, are to develop, promulgate, review or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, pursuant to Section 20 of the DPA, the PIC must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal data;

WHEREAS, under Section 22 of the DPA, 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 is secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the NPC;

WHEREAS, under Section 23 of the DPA, the NPC may issue guidelines relating to access by agency personnel to sensitive personal information;

WHEREFORE, the abovementioned premises considered, the NPC hereby issues this Circular governing the security of personal data.

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 DPA, its IRR, and other relevant issuances of the NPC.

SECTION 2. ***Purpose.*** **-** This Circular aims to provide updated requirements for the security of personal data processed by a PIC or Personal Information Processor (PIP). Due to the general nature of this Circular, a PIC or PIP may implement more detailed or stricter policies and procedures that reflect industry-specific operating requirements.

SECTION 3. ***Definition of Terms***. **–** Terms used in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms are defined as follows:

A. "*Acceptable Use Policy*" refers to a document or set of rules stipulating controls or restrictions that personnel of a PIC or PIP must agree to for access to the network, facilities, equipment, or services of such PIC or PIP;
B. "*Access Control Policy*" refers to a document or set of rules that defines how access to information is managed, including who may access specific information and under what circumstances;
C. *"Automated Processing"* generally refers to the use of automated means, such as algorithms or computer systems, in carrying out processing activities without human intervention;
D. "*Business Continuity*" refers to the capability of a PIC or PIP to continue the delivery of products or services at acceptable pre-defined levels following disruptive events;
E. "*Business Continuity Plan*" refers to documented procedures that guide a PIC or PIP to respond, recover, resume, and restore systems and processes to a pre-defined level of operation following disruptive events;
F. *"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;
G. "*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;
H. "*Disruptive Events*" refer to any anticipated or unanticipated occurrence or change which interrupts planned activities, operations, or functions;
I. "*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;
J. "*Government Agency*" refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, Constitutional Commissions, local government units, government-owned and controlled corporations, government financial institutions, and state colleges and universities;
K. *"National Computer Emergency Response Team (NCERT)"* refers to the highest body for cybersecurity-related activities;
L. *"Off-The-Shelf Software"* refers to a software product that is ready-made and commercially available for sale, lease, or license to the general public;

M. *"Password Policy"* refers to a document or set of rules that passwords must satisfy to increase the security and privacy of electronic devices;
N. *"Privacy Engineering"* refers to the integration of privacy concerns into engineering practices for systems and software engineering life cycle processes;
O. "*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;
P. "*Privacy-by-Default*" refers to the principle according to which the PIC/PIP ensures that only data necessary for each specific purpose of processing is processed by default, without the intervention of the data subject;
Q. *"Privacy Management Program (PMP)"* refers to a holistic program towards privacy and data protection and is important for a PIC or PIP involved in the processing of personal data. It is intended to embed privacy and data protection in the strategic framework and daily operations of a PIC or its PIP;
R. "*Security Clearance*" refers to the permission granted to an individual to access information based on the given level of access;
S. *"System Management Tool"* refers to a software system that facilitates the administration of user passwords and access rights;
T. "*Telecommuting*" refers to work from an alternative workplace with the use of telecommunications or computer technologies.

SECTION 4. ***General Obligations.*** **–** **A** PIC and its PIP shall fulfill the following responsibilities:

A. Designate and register its Data Protection Officer (DPO) with the NPC, taking into account the provisions of the DPA, its IRR, its amendments, and any other issuances of the NPC on the designation and registration of a DPO;
B. Register its data processing systems with the NPC according to the provisions of the DPA, its IRR, its amendments, and any other issuances of the NPC on the registration of data processing systems;
C. Create an inventory of all its data processing systems and activities taking into account Section 26 (c) and (e) of the IRR;
D. Conduct a Privacy Impact Assessment (PIA) on the processing of personal data: *Provided*, that such assessment shall be updated as necessary (e.g., new features or major changes in processing, new regulations, new contracts entered by the PIC, or changes in its PIP). Both previously assessed controls and those newly identified through recent PIAs shall be monitored, evaluated, updated, and incorporated as a component of a PIC's Privacy Management Program;
E. Set a Privacy Management Program, taking into account the following:
    1. Organizational commitment and leadership responsibilities for data privacy;
    2. Control framework for the development of privacy policies and implementation of data protection measures; and
    3. Oversight and continuous improvement of controls.
F. Periodically train employees, agents, personnel, or representatives on privacy and data protection policies;

G. Comply with the NPC's orders when the PIC and its PIP's privacy and data protection policies are subject to review and assessment in terms of compliance with the requirements of the DPA, its IRR, and all relevant issuances of the NPC.

SECTION 5. ***Privacy Impact Assessment (PIA).*** **-** A PIA should be undertaken for every processing system of a PIC or PIP that involves personal data.

The PIA shall include the following:

A. a data inventory identifying:
    1. the amount and type of personal data held by the PIC and its PIP, if any, including records of its own personnel;
    2. list of all information repositories holding personal data, including location;
    3. type of media used for storing the personal data;
    4. risks associated with the processing of personal data; and
    5. processing operations for the entire personal data life cycle, from collection to disposal or destruction;
B. a systematic description of the personal data being processed or to be processed, including the purposes for such processing, anticipated purposes, and their corresponding lawful bases;
C. an assessment of the general data privacy principles in relation to the processing;
D. a holistic assessment of the risks to the rights and freedoms of a data subject; and
E. an assessment of risks to the confidentiality, integrity, and availability of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

The PIA need not be submitted to the NPC, but it shall be made available by the PIC upon the NPC's request arising from investigations or compliance checks.

SECTION 6. ***Control Framework for Data Protection***. **-** The risks identified in the PIA 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 volume of personal data being processed;
C. Current data privacy best practices in a specific industry;
D. Cost of security implementation; and
E. Purpose and extent of data sharing or outsourcing agreements and their attendant risks.

RULE II.
EMBEDDING PRIVACY-BY-DESIGN AND PRIVACY-BY-DEFAULT

SECTION 7. ***Privacy-By-Design and Privacy-By-Default.*** — A PIC or PIP shall consider Privacy-By-Design principles in its processing activities and enable Privacy-By-Default in its data processing systems without requiring any action from its data subjects.

Further, a PIC or PIP must also conduct a PIA on its Off-The-Shelf Software, solutions, or data processing systems, as outlined in Section 5 of this Circular.

Any functions that lack a lawful basis for processing or are incompatible with the general data privacy principles, must be switched off or deactivated.

SECTION 8. ***Privacy Engineering.*** **-** A PIC or PIP should incorporate data privacy requirements throughout the development and implementation of data processing systems.

RULE III.
STORAGE OF PERSONAL DATA

SECTION 9. ***General Rule.*** **-** A PIC or PIP must store personal information in a form that permits the identification of data subjects for only as long as necessary for the specific purpose for which it was initially processed.

In order to ensure that personal data is not kept longer than necessary, the PIC should establish and document retention periods in a policy. This Retention Policy, which defines retention periods, must be reviewed periodically and amended as necessary. The PIC should inform data subjects about the Retention Policy, including its changes.

SECTION 10. ***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 of the NPC.

SECTION 11. ***Protection of Personal Data.*** **-** All personal data that are processed must be adequately protected through industry standards and best practices.

Passwords or passphrases used to access personal data should be of sufficient strength and uniqueness to deter password attacks. Each PIC or PIP shall issue and enforce a Password Policy.

RULE IV.
ACCESS TO PERSONAL DATA

SECTION 12. ***Access to or Modification of Databases.*** **-** Personal data stored in databases under the control of the PIC may only be accessed or modified using authorized software programs either by the PIC or by its PIP. Authorized software programs are those that are either licensed or owned by the PIC or PIP. Such restriction is necessary to protect the confidentiality, integrity, and availability of personal data.

SECTION 13. ***Restricted Access.*** **-** A PIC or PIP shall implement an Access Control Policy to ensure that only authorized personnel can access personal data on a "need to know" basis. Further, a PIC or PIP shall provide other mechanisms, such as authentication methods and regular monitoring, to limit access to only authorized personnel.

A PIC must ensure that access to personal data is strictly regulated by issuing a security clearance or its equivalent only to its authorized personnel. Any processing performed by a PIP must be covered by the appropriate and necessary agreement that contains an equivalent of this provision as well as other provisions required under the IRR.

A copy of the appropriate security clearance or its equivalent must be filed with the DPO of the PIC.

SECTION 14. ***PIP Access***. **-** Access to personal data by a PIP engaged by a PIC shall be governed by strict procedures contained in formal contracts or other legal acts, and the provisions of such must comply with the DPA, its IRR, and all applicable issuances by the NPC. The contractual terms and undertakings stated may be considered by the NPC when evaluating the security measures implemented by the PIC.

SECTION 15. ***Acceptable Use Policy***. **-** A PIC or PIP shall have an updated Acceptable Use Policy regarding the use by PIC or PIP's personnel of information and communications technology. The PIC or PIP shall explain the policy to all personnel who use such technology in relation to their functions. Each user shall agree to the policy and, for this purpose, sign the appropriate agreement before being allowed access to and use of the technology.

SECTION 16. ***Online Access to Personal Data.*** **-** A PIC or PIP shall implement secure authentication mechanisms, such as multifactor authentication or secure encrypted links, when providing personnel online access to sensitive personal information, privileged information, and a high volume of personal data. Such user access rights and authentication mechanisms must be defined and controlled by a System Management Tool.

SECTION 17. ***Authorized Devices.*** **-** A PIC or PIP shall ensure that only known devices, properly configured to the PIC's or PIP's security standards, are authorized to access personal data. The PIC or PIP shall also establish solutions that only allow authorized media to be used on its computer equipment. These measures include but are not limited to the following:

1. Setting a group policy to allow certain types of devices to be connected[1];
2. Use of endpoint security solutions;[2] and
3. Restricting access to USB ports.[3]

SECTION 18. ***Remote Disconnection or Deletion.*** A PIC shall employ technology solutions that enable remote disconnection or data deletion on mobile devices owned by the PIC when they are lost or compromised. In addition, PICs shall establish a notification process in cases of mobile device loss to ensure swift and appropriate actions toward safeguarding personal data contained therein.

SECTION 19. ***Physical Filing System.*** **-** If personal data is stored in any physical media, such as a paper-based filing system, a PIC or PIP shall maintain a log, from which it can be ascertained which file was accessed, including when, where, and by whom. Such log shall

[1] vinaypamnani-msft, "Manage Device Installation with Group Policy - Windows Client Management," August 10, 2023, https://learn.microsoft.com/en-us/windows/client-management/client-tools/manage-device-installation-with-group-policy.
[2] "USB Security Software - USB Port Blocker & Analyzer | SolarWinds," accessed October 24, 2023, https://www.solarwinds.com/security-event-manager/use-cases/usb-security-analyzer.
[3] Azharuddin@TWC, "How to Enable or Disable USB Ports in Windows 11/10," The Windows Club, June 28, 2021, https://www.thewindowsclub.com/disable-enable-usb-windowunlock-pen-drive-at-office-or-school-computer.

also indicate whether copies of the file were made. The PIC or PIP shall regularly review the log records, including all applicable procedures.

SECTION 20. ***Personal Data Sharing Agreements***. **-** Access by other parties to personal data under the control or custody of a PIC shall be governed by the DPA, its IRR, and the NPC's relevant issuances on Data Sharing Agreements.

RULE V.
BUSINESS CONTINUITY

SECTION 21. ***Business Continuity Management.*** **-** A PIC or PIP must have a Business Continuity Plan to mitigate potential disruptive 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 assessment, crisis communications plan, and telecommuting policy, among others; and
iii. Contact information and other business-critical matters, e.g., electrical supply, building facilities, Information and Communications Technology (ICT) assets.

SECTION 22. ***Telecommuting***. **-** The adoption of telecommuting or other alternative work arrangements is a viable strategy to continuously operate and provide essential goods and services. With this, a PIC or PIP shall set, in accordance with applicable laws, rules and regulations, its policy on alternative work arrangements, and communicate it to concerned stakeholders. Security measures in alternative work arrangements shall be considered by the PIC or PIP. These measures include:

i. Training on the limitations on use of company-issued computing devices with secure configuration of the PIC's Information and Communications Technology (ICT) assets to protect against security risks and cyberthreats such as unauthorized access, malware, data loss, and theft;
ii. Best password management and secured practices in managing online accounts, computers, mobile phones, and network appliances; and
iii. Periodic trainings on data privacy, cybersecurity, and online productivity, among others.

RULE VI.
TRANSFER OF PERSONAL DATA

SECTION 23. ***Emails.*** **-** A PIC or PIP that transfers personal data by email must ensure that the data is adequately protected and use secure transmission and reception of email messages, including attachments. Where appropriate, a PIC or PIP may utilize systems that scan outgoing emails and attachments for keywords that would indicate the presence of personal data and, if applicable, prevent its transmission.

SECTION 24. ***Personal Productivity Software.*** **-** A PIC or PIP that do not have any security or access controls when using personal productivity software, shall, when reasonable and appropriate, implement security controls to prevent its personnel from printing or copying personal data to personal productivity software such as word processors and spreadsheets.

SECTION 25. ***Removable or Portable Storage Media.*** **-** The use of removable or portable storage media, such as compact discs (CD), digital versatile discs (DVD), and Universal Serial Bus (USB) flash drives for processing personal data, shall be regulated: *Provided*, that if such mode of transfer is unavoidable or necessary, the files inside the removable or portable storage media shall be encrypted.

SECTION 26. ***Fax Machines.*** **-** Facsimile technology shall not be used for transmitting documents containing personal data.

SECTION 27. ***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 the authorized representative of the addressee: *Provided*, that similar safeguards shall be adopted relative to documents or media transmitted between offices or personnel of the PIC and its PIP.

RULE VII.
GUIDELINES FOR DISPOSAL OF PERSONAL DATA

SECTION 28. ***Disposal and Destruction of Personal Data***. **-** In establishing policies and procedures for disposal of personal data, a PIC or PIP shall take into consideration the following:

1. Retention period of data;
2. Jurisdiction-specific laws, regulations, and existing contracts;
3. Identification of relevant de-identification, anonymization, or deletion techniques for specific types of data; and
4. Required documentation before the deletion, de-identification, or anonymization of personal information.

SECTION 29. ***Logs Retention.*** **–** A PIC or a PIP shall retain logs as long as deemed necessary and appropriate based on best practices and industry standards. In determining the appropriate retention period, the PIC shall consider the type of log and its corresponding use. Security logs that record information about authentication attempts and security incidents shall be retained for longer periods than general system logs:

A. In the event of a security incident or data breach, logs may need to be retained for a longer period to support investigations and digital forensic analysis. PICs shall retain logs related to incidents for a specified period required by the NPC, even if it exceeds their retention policies; and
B. PICs shall implement backup and archive mechanisms for their logs. Backup copies may be retained for shorter periods, while archived copies can be stored for a longer duration.

SECTION 30. ***Procedures for Disposal and Destruction.*** **-** Procedures must be established to ensure secure and proper disposal and destruction of personal data that would render further processing impossible. These include:

1. Disposing and destroying personal data, regardless of how such files are stored;
2. Electronically disposing or destroying personal data in storage media which involve the use of degaussers, erasers, encryption, or secure wiping programs as applicable;
3. Physically disposing or destroying storage media used to store personal data such as disk servers, hard or solid-state drives, portable storage drives, such as disks, flash drives and memory cards, read-only memory storage in mobile phones when they reach the end-of-life;
4. Disposing and destroying personal data in paper documents which involve the use of paper shredders that would render shredded paper documents into small pieces that cannot be reassembled; and
5. Disposing personal data stored offsite.

SECTION 31. ***Personal Data Disposal Service Provider.*** **-** A PIC may engage a PIP to carry out the disposal of personal data under its control: *Provided,* that the PIP shall contractually agree to the PIC's data protection procedures and ensure that the confidentiality of all personal data is preserved.

RULE VIII.
MISCELLANEOUS PROVISIONS

SECTION 32. ***Threat monitoring and vulnerability management.*** **-** A PIC or a PIP shall continuously adapt security measures to dynamically respond to the evolving security threat landscape. This includes identifying threats based on authoritative sources of threat information (e.g., NCERT), integrating relevant threats into the PIA to determine if these lead to new unacceptable security or privacy risks, and proposing corrective actions to such threats.

SECTION 33. ***Personal Data Breach Management.*** **-** In case of a data breach or security incident, a PIC shall comply with the requirements of the NPC's issuance on breach management.

SECTION 34. ***Audit***. **–** In certain cases**,** independent verification or certification by a reputable third party of a PIC or, where applicable, its PIP, may be accepted by the NPC: *Provided*, that the findings of an independent verification or certification by a third-party does not preclude the NPC from performing its regulatory functions pursuant to the relevant issuances of the NPC.

SECTION 35. ***Penalties***. **-** A PIC or PIP that violates the provisions of this Circular, 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 NPC'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 36. ***Review***. **-** This Circular shall be subject to regular review by the NPC.

SECTION 37. - ***Transitory Period***. **-** A PIC shall be given a transitory period of twelve (12) months from the effectivity of this Circular to comply with the requirements provided herein.

SECTION 38. ***Separability Clause***. **-** If any portion or provision of this Circular is declared null and void or unconstitutional, then the other provisions not affected thereby shall continue to be in force and effect.

SECTION 39. ***Repealing Clause***. **-** This Circular expressly repeals NPC 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 40. ***Effectivity***. **-** These Rules shall take effect fifteen (15) days after its publication in a newspaper of general circulation.

Approved:

SGD
JOHN HENRY D. NAGA
Privacy Commissioner

SGD
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

SGD
NERISSA N. DE JESUS
Deputy Privacy Commissioner