Republic of the Philippines
National Privacy Commission
privacycommissioner@privacy.gov.ph

NPC Circular 16-01

DATE : **10 October 2016**

TO : **ALL HEADS OF GOVERNMENT BRANCHES, BODIES OR ENTITIES, INCLUDING NATIONAL GOVERNMENT AGENCIES, BUREAUS OR OFFICES, CONSTITUTIONAL COMMISSIONS, LOCAL GOVERNMENT UNITS, GOVERNMENT-OWNED AND –CONTROLLED CORPORATIONS, STATE COLLEGE AND UNIVERSITIES**

SUBJECT : **SECURITY OF PERSONAL DATA IN GOVERNMENT AGENCIES**

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, also 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 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 in the private sector are secured and protected;

WHEREAS, pursuant to Section 7 of the Data Privacy Act of 2012, 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 Section 22 of the Data Privacy Act of 2012, 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;

WHEREAS, under Section 23 of the Data Privacy Act of 2012, the Commission may issue guidelines relating to access by agency personnel to sensitive personal information;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides that, among the Commission's functions, is to develop, promulgate, review or amend rules and regulations for the effective implementation of the Act;

WHEREFORE, in consideration of these premises, the National Privacy Commission hereby issues this Circular governing the security of personal data in government agencies.

RULE I.
GENERAL PROVISIONS

SECTION 1. ***Scope***. These Rules shall apply to all government agencies engaged in the processing of personal data.

SECTION 2. ***Purpose.*** These Rules are hereby issued to assist government agencies engaged in the processing of personal data to meet their legal obligations under Republic Act No. 10173, also known as the Data Privacy Act of 2012, and its corresponding Implementing Rules and Regulations.

A government agency may use these Rules to issue and implement more detailed policies and procedures, which reflect its specific operating requirements.

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

A. "Acceptable Use Policy" shall refer to a document or set of rules stipulating controls or restrictions that agency personnel must agree to for access to their agency's network, facilities, equipment, or services;

B. "Act" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012 (DPA);

C. "Agency Personnel" refers to all officials, officers, employees or consultants of a government agency, including those covered by job orders or contracts of services;

D. "Commission" refers to the National Privacy Commission (NPC);

E. "Data Center" refers to a centralized repository, which may be physical or virtual, may be analog or digital, used for the storage, management, and dissemination of data including personal data;

F. "Data Protection Officer" refers to an individual designated by the head of agency to be accountable for the agency's compliance with the Act: *Provided*, that the individual must be an organic employee of the government agency: *Provided further*, that a government agency may have more than one data protection officer;

G. "Government Agency" refers to a government branch or body or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

H. "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;

I. "Implementing Rules and Regulations" or "IRR" shall pertain to Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

J. "Personal Data" shall refer to all types of personal information, including those pertaining to agency personnel;

K. "Privacy Impact Assessment" is a process undertaken and used by a government agency to evaluate and manage privacy impacts;

L. "System Management Tool" is a software system that facilitates the administration of user passwords and access rights.

SECTION 4. ***General Obligations*****.** A government agency engaged in the processing of personal data shall observe the following duties and responsibilities:

A. through its head of agency, designate a Data Protection Officer;

B. conduct a Privacy Impact Assessment for each program, process or measure within the agency that involves personal data, *Provided*, that such assessment shall be updated as necessary;

C. create privacy and data protection policies, taking into account the privacy impact assessments, as well as Sections 25 to 29 of the IRR;

D. conduct a mandatory, agency-wide training on privacy and data protection policies once a year: *Provided*, that a similar training shall be provided during all agency personnel orientations.

E. register its data processing systems with the Commission in cases where processing involves personal data of at least one thousand (1,000) individuals, taking into account Sections 46 to 49 of the IRR;

F. cooperate with the Commission when the agency's privacy and data protection policies are subjected to review and assessment, in terms of their compliance with the requirements of the Act, its IRR, and all issuances by the Commission.

SECTION 5. ***Privacy Impact Assessment***. A government agency engaged in the processing of personal data shall ensure that its conduct of a privacy impact assessment is proportionate or consistent with the size and sensitivity of the personal data being processed, and the risk of harm from the unauthorized processing of that data.

The Privacy Impact Assessment shall include the following:

A. a data inventory identifying:

   1.) the types of personal data held by the agency, including records of its own employees;
   2.) list of all information repositories holding personal data, including their location;
   3.) types of media used for storing the personal data; and
   4.) risks associated with the processing of the personal data;

B. a systematic description of the processing operations anticipated and the purposes of the processing, including, where applicable, the legitimate interest pursued by the agency;

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 data subjects.

SECTION 6. ***Control Framework for Data Protection***. The risks identified in the privacy impact assessment 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 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.

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 complexity of its operations;
C. current data privacy best practices; and
D. cost of security implementation.

For agencies that process the personal data records of more than one thousand (1,000) individuals, including agency personnel, the Commission recommends the use of the ISO/IEC 27002 control set as the minimum standard to assess any gaps in the agency's control framework.

RULE II.
STORAGE OF PERSONAL DATA

SECTION 7. ***General Rule.*** Personal data being processed by a government agency shall be stored in a data center, which may or may not be owned and controlled by such agency: *Provided*, that the agency must be able to demonstrate to the Commission how its control framework for data protection, and/or, 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 agency to submit its contract with its service provider for review.

SECTION 8. ***Encryption of Personal Data.*** All personal data that are digitally processed must be encrypted, whether at rest or in transit. For this purpose, the Commission recommends Advanced Encryption Standard with a key size of 256 bits (AES-256) as the most appropriate encryption standard.

Passwords or passphrases used to access personal data should be of sufficient strength to deter password attacks. A password policy should be issued and enforced through a system management tool.

SECTION 9. ***Restricted Access***. Access to all data centers owned and controlled by a government agency shall be restricted to agency 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 agency management regularly.

SECTION 10. ***Service Provider as Personal Information Processor***. When a government agency engages a service provider for the purpose of storing personal data under the agency's control or custody, the service provider shall function as a personal information processor and comply with all the requirements of the Act, its IRR and all applicable issuances by the Commission.

SECTION 11. ***Audit***. The Commission reserves the right to audit a government agency'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 12. ***Recommended Independent Verification or Certification***. The Commission recommends ISO/IEC 27018 as the most appropriate certification for the service or function provided by a service provider under this Rule.

SECTION 13. ***Archives***. The requirements of this Rule shall also apply to personal data that a government agency has stored for archival purposes.

RULE III.
AGENCY ACCESS TO PERSONAL DATA

SECTION 14. ***Access to or Modification of Databases***. Only programs developed or licensed by a government agency shall be allowed to access and modify databases containing the personal data under the control or custody of that agency.

SECTION 15. ***Security Clearance***. A government agency shall strictly regulate access to personal data under its control or custody. It shall grant access to agency personnel, through the issuance of a security clearance by the head of agency, 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 agency's Data Protection Officer.

SECTION 16. ***Contractors, Consultants and Service Providers***. Access to personal data by independent contractors, consultants, and service providers engaged by a government agency shall be governed by strict procedures contained in formal contracts, which provisions must comply with the Act, its IRR, and all applicable issuances by the Commission. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance.

SECTION 17. ***Acceptable Use Policy***. Each government agency shall have an up-to-date Acceptable Use Policy regarding the use by agency personnel of information and communications technology. The policy shall be explained to all agency 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 used of the technology.

SECTION 18. ***Online Access to Personal Data.*** Agency 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 19. ***Local Copies of Personal Data Accessed Online.*** A government agency shall adopt and utilize technologies that prevent personal data accessible online to authorized agency

personnel from being copied to a local machine. The agency shall also provide for the automatic deletion of temporary files that may be stored on a local machine by its operating system.

Where possible, agency 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 government agency may also consider prohibiting the use of cameras in areas where personal data is displayed or processed.

SECTION 20. ***Authorized Devices.*** A government agency shall ensure that only known devices, properly configured to the agency's security standards, are authorized to access personal data. The agency shall also put in place solutions, which only allow authorized media to be used on its computer equipment.

SECTION 21. ***Remote Disconnection or Deletion.*** A government agency shall adopt and use technologies that allow the remote disconnection of a mobile device owned by the agency, or the deletion of personal data contained therein, in event such mobile device is lost. A notification system for such loss must also be established.

SECTION 22. ***Paper-based Filing System.*** If personal data is stored in paper files or any physical media, the government agency 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. Agency management shall regularly review the log records, including all applicable procedures.

SECTION 23. ***Personal Data Sharing Agreements***. Access by other parties to personal data under the control or custody of a government agency shall be governed by data sharing agreements that will be covered by a separate issuance of the Commission.

RULE IV.
TRANSFER OF PERSONAL DATA

SECTION 24. ***Emails.*** A government agency that transfers personal data by email must either ensure that the data is encrypted, or use a secure email facility that facilitates the encryption of the data, including any attachments. Passwords should be sent on a separate email. It is also recommended 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 25. ***Personal Productivity Software.*** A government agency shall implement access controls to prevent agency 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 26. ***Portable Media.*** A government agency that uses portable media, such as disks or USB drives, to store or transfer personal data must ensure that the data is encrypted. Agencies that use laptops to store personal data must utilize full disk encryption.

SECTION 27. ***Removable Physical media.*** Where possible, the manual transfer of personal data, such as through the use of removable physical media like compact discs, shall not be allowed: *Provided*, that if such mode of transfer is unavoidable or necessary, authentication technology, such as one-time PINs, shall be implemented.

SECTION 28. ***Fax Machines.*** Facsimile technology shall not be used for transmitting documents containing personal data.

SECTION 29. ***Transmittal.*** A government agency that transmits documents or media containing personal data by mail or post shall make use of registered mail or, where appropriate, guaranteed parcel post service. 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 within the agency.

RULE V.
DISPOSAL OF PERSONAL DATA

SECTION 30. ***Archival Obligations.*** A government agency must be aware of its legal obligations as set out in Republic Act No. 9470, also known as the National Archives of the Philippines Act of 2007. Personal data records, as well as incoming and outgoing emails, of enduring value may be archived pursuant to such Act.

SECTION 31. ***Procedures.*** Procedures must be established regarding:

A. disposal of files that contain personal data, whether such files are stored on paper, film, optical or magnetic media;
B. 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
C. disposal of personal data stored offsite.

SECTION 32. ***Third-Party Service Providers.*** A government agency 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 agency's data protection procedures and ensure that the confidentiality of all personal data is protected.

RULE VI.
MISCELLANEOUS PROVISIONS

SECTION 33. ***Data Breach Management.*** The appropriate guidelines for managing data breaches will be the subject of a separate issuance by the Commission.

SECTION 34. ***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 a schedule to be published by the Commission.

Failure to comply with the provisions of this Circular may be a ground for administrative and disciplinary sanctions against any erring public 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 35. ***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 36. ***Transitory Period***. Government agencies shall be given a period of one (1) year transitory period from the effectivity of these Rules to comply with the requirements provided herein.

SECTION 37. ***Separability Clause***. If any portion or provision of these Rules is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 38. ***Repealing Clause***. All other rules, regulations, and issuances contrary to or inconsistent with the provisions of these Rules are deemed repealed or modified accordingly.

SECTION 39. ***Effectivity***. These Rules shall take effect fifteen (15) days after its publication in the Official Gazette.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATDU
Deputy Privacy Commissioner

(Sgd.) DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner