



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular 17-01

DATE : 31 July 2017

TO : ALL PERSONAL INFORMATION CONTROLLERS AND PERSONAL INFORMATION PROCESSORS

SUBJECT : REGISTRATION OF DATA PROCESSING SYSTEMS AND NOTIFICATIONS REGARDING AUTOMATED DECISION-MAKING

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 (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 also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secure and protected;

WHEREAS, Section 16 of the DPA and Section 34 of its Implementing Rules and Regulations (IRR) provide that data subjects shall be furnished with and given access to their personal data that are being processed in data processing systems, as well as the purpose, scope, method, and manner of such processing, including the existence of automated decision-making;

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 by personal information controllers (PICs) with the provisions thereof, publishing a compilation of an agency's system of records and notices, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal data, in coordination with other government agencies and private entities;

WHEREAS, Section 9 of the IRR provides that, among the NPC's functions, is to develop, promulgate, review, or amend rules and regulations for the effective implementation of the DPA;

WHEREAS, Section 24 of the DPA states that, when entering into any contract that may involve accessing or requiring sensitive personal information from at least one thousand (1,000) individuals, a government agency shall require the contractor and its employees to register their personal information processing system with the NPC in accordance with the DPA and to comply with the law's provisions. Furthermore, Section 14 of the law mandates that personal information processors (PIPs) shall also comply with all requirements of the DPA and other applicable laws;

WHEREAS, in line with Sections 46 and 47 of the IRR, a PIC or PIP that employs fewer than two hundred fifty (250) persons shall not be required to register unless the processing it carries out is likely to pose a risk to the rights and freedoms of data subjects, is not occasional, or includes sensitive personal information of at least one thousand (1,000) individuals. Moreover, Section 48 thereof declares that a PIC carrying out any automated processing operation that is intended to serve a single or several related purposes must notify the NPC when said operation becomes the sole basis for making decisions about a data subject, and when such decision would significantly affect the data subject;

WHEREFORE, in consideration of these premises, the NPC hereby issues this Circular governing the registration of data processing systems and notifications regarding automated decision-making:

RULE I. PRELIMINARY PROVISIONS

SECTION 1. *Scope.* The provisions of this Circular shall apply to any natural or juridical person in the government or private sector processing personal data and operating in the Philippines, subject to the relevant provisions of the DPA, its IRR, and other applicable issuances of the NPC.

SECTION 2. *Purpose.* This Circular establishes the framework for registration of data processing systems in the Philippines and imposes other requirements for the purpose of achieving the following objectives:

- A. ensure that PICs and PIPs keep a record of their data processing activities;
- B. make information about data processing systems operating in the country accessible to both the Commission, for compliance monitoring, and data subjects, to facilitate the exercise of their rights under the DPA; and
- C. promote transparency and public accountability in the processing of personal data.

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

- A. “Act” or “DPA” refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- B. “Automated Decision-making” refers to a wholly or partially automated processing operation that serves as the sole basis for making decisions that would significantly affect a data subject. It includes the process of profiling based on an individual’s economic situation, political or religious beliefs, behavioral or marketing activities, electronic communication data, location data, and financial data, among others;
- C. “Commission” or “NPC” refers to the National Privacy Commission;
- D. “Compliance Officer for Privacy” or “COP” refers to an individual that performs some of the functions of a DPO, as provided in NPC Advisory No. 17-01;
- E. “Core Activity” refers to a key operation or process carried out by a PIC or PIP to achieve its mandate or function: *Provided*, that processing of personal data forms an integral and necessary part of such operations or processes;
- F. “Data Processing System” refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;
- G. “Data Protection Officer” or “DPO” refers to an individual designated by the head of agency or organization to be accountable for 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 have more than one DPO;
- H. “Data sharing” is the disclosure or transfer to a third party of personal data under the control or custody of a PIC: *Provided*, that a PIP may be allowed to make such disclosure or transfer if it is upon the instructions of the PIC concerned.

The term excludes outsourcing, or the disclosure or transfer of personal data by a PIC to a PIP;

- I. “Data Subject” refers to an individual whose personal, sensitive personal, or privileged information is processed;

- J. "Encryption Method" refers to the technique that renders data or information unreadable, ensures that it is not altered in transit, and verifies the identity of its sender;
- K. "Filing system" refers to any set of information relating to a natural or juridical person to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible;
- L. "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, state colleges and universities;
- M. "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;
- N. "Head of organization" refers to the head or decision-making body of a private entity or organization;
- O. "Information and Communications System" refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages, or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document;
- P. "IRR" refers to the Implementing Rules and Regulations of the DPA;
- Q. "Personal data" refers to all types of personal information;
- R. "Personal information" refers to any information, whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;
- S. "Personal information controller" or "PIC" refers to a natural or juridical person, or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. The term excludes:

1. a natural or juridical person, or any other body, who performs such functions as instructed by another person or organization; or
2. a natural person who processes personal data in connection with his or her personal, family, or household affairs;

There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

- T. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;
- U. "Private entity" or "organization" refers to any natural or juridical person that is not a unit of the government, including, but not limited to, a corporation, partnership, company, non-profit organization or any other legal entity;
- V. "Privileged information" refers to all forms of data, which, under the Rules of Court and other pertinent laws, constitute privileged communication;
- W. "Profiling" refers to any form of automated processing of personal data consisting of the use of personal data, such as a individual's economic situation, political or religious beliefs, behavioral or marketing activities, personal preferences, electronic communication data, location data, and financial data, among others, in order to evaluate, analyze, or predict his or her performance, qualities, and behavior, among others;
- X. Sensitive personal information refers to personal information:
1. about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
 2. about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
 3. issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and
 4. specifically established by an executive order or an act of Congress to be kept classified.

SECTION 4. *General Principles.* This Circular shall be governed by the following general principles:

- A. Registration of its data processing systems with the Commission shall be one of the means through which a PIC or PIP demonstrates its compliance with the DPA, its IRR, and other relevant issuances of the NPC.
- B. Registration information submitted by a PIC or PIP to the Commission are presumed to contain all required information on its data processing systems that are active or existing during the validity of such registration. Any information excluded therefrom are deemed nonexistent.
- C. Unless otherwise provided in this Circular, any information, file, or document submitted by a PIC or PIP to the Commission shall be kept confidential.
- D. Any doubt in the interpretation of the provisions of this Circular shall be liberally interpreted in a manner that would uphold the rights and interests of data subjects.

RULE II.
REGISTRATION OF DATA PROCESSING SYSTEMS

SECTION 5. *Mandatory Registration.* A PIC or PIP shall register its data processing systems if it is processing personal data and operating in the country under any of the following conditions:

- A. the PIC or PIP employs at least two hundred fifty (250) employees;
- B. the processing includes sensitive personal information of at least one thousand (1,000) individuals;
- C. the processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:
 - 1.) information that would likely affect national security, public safety, public order, or public health;
 - 2.) information required by applicable laws or rules to be confidential;
 - 3.) vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP;
 - 4.) automated decision-making; or
 - 5.) profiling;

- D. the processing is not occasional: *Provided*, that processing shall be considered occasional if it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional:

In determining the existence of the foregoing conditions, relevant factors, such as the number of employees, or the records of individuals whose sensitive personal information are being processed, shall only be considered if they are physically located in the Philippines.

Data processing systems that involve automated decision-making shall, in all instances, be registered with the Commission. For all other data processing systems operating under the conditions set out in subsections C and D, the Commission shall determine the specific sectors, industries, or entities that shall be covered by mandatory registration. Appendix 1 of this Circular shall feature the initial list. It shall be regularly reviewed and may be updated by the Commission through subsequent issuances.

SECTION 6. *Voluntary Registration.* An application for registration by a PIC or PIP whose data processing system does not operate under any of the conditions set out in the next preceding Section shall be accepted as a voluntary registration.

SECTION 7. *When to Register.* A PIC or PIP covered by this Circular shall register its personal data processing system within two (2) months of the commencement of such system.

SECTION 8. *Authority to Register.* A PIC or PIP shall file its application for registration through its designated or appointed DPO: *Provided*, that where a PIC or PIP has several DPOs, only one shall be authorized to file the application of the PIC or PIP: *Provided further*, that where the same individual assumes the role of DPO for two or more PICs or PIPs, he or she shall be allowed to file the applications of all his or her principals.

SECTION 9. *Registration Process.* A PIC or PIP shall register through the Commission's official website in two (2) phases:

- A. *Phase I.* A PIC or PIP, through its DPO, shall accomplish the prescribed application form, and submit the same to the Commission together with all supporting documents. Upon review and validation of the submission, the Commission shall provide the PIC or PIP via email an access code, which shall allow it to proceed to Phase II of the registration process.

- B. *Phase II.* Using the access code provided by the Commission, a PIC or PIP shall proceed to the online registration platform and provide all relevant information regarding its data processing systems. The Commission shall notify the PIC or PIP via email to confirm the latter's successful completion of the registration process:

Provided, that registration may be done in person at the office of the Commission in the event that online access is not available.

SECTION 10. *Application Form.* An application for registration filed by a PIC or PIP must be duly-notarized and accompanied by the following documents:

- A. For government agencies:
 - 1.) certified true copy of the Special/Office Order, or any similar document, designating or appointing the DPO of the PIC or PIP; and
 - 2.) where applicable, a copy of the charter of the government entity, or any similar document identifying its mandate, powers, and/or functions.

- B. For private entities:
 - 1.) duly-notarized Secretary's Certificate authorizing the appointment or designation of DPO, or any other document that demonstrates the validity of the appointment or designation.
 - 2.) certified true copy of the following documents, where applicable:
 - a.) General Information Sheet or any similar document;
 - b.) Certificate of Registration (SEC Certificate, DTI Certification of Business Name or Sole Proprietorship) or any similar document; and/or
 - c.) Franchise, license to operate, or any similar document.

SECTION 11. *Online Registration Platform.* In the Commission's online registration platform, a PIC or PIP shall provide the following registration information:

- A. name and contact details of the PIC or PIP, head of agency or organization, and DPO;
- B. purpose or mandate of the government agency or private entity;
- C. identification of all existing policies relating to data governance, data privacy, and information security, and other documents that provide a general description of privacy and security measures for data protection;

- D. attestation regarding certifications attained by the PIC or PIP, including its relevant personnel, that are related to personal data processing;
- E. brief description of data processing system or systems:
 - 1.) name of the system;
 - 2.) purpose or purposes of the processing;
 - 3.) whether processing is being done as a PIC, PIP, or both;
 - 4.) whether the system is outsourced or subcontracted, and if so, the name and contact details of the PIP;
 - 5.) description of the category or categories of data subjects, and their personal data or categories thereof;
 - 6.) recipients or categories of recipients to whom the personal data might be disclosed; and
 - 7.) whether personal data is transferred outside of the Philippines;
- F. notification regarding any automated decision-making operation.

This same set of information shall be given when registration is done in person at the office of the Commission.

SECTION 12. *Certificate of Registration.* The Commission shall issue a certificate of registration in favor of a PIC or PIP that has successfully completed the registration process: *Provided*, that such certificate shall only be considered as proof of registration and not a verification of the contents thereof.

SECTION 13. *Validity.* A certificate of registration, once issued, shall be valid only until the 8th day of March of the next following year: *Provided*, that the certificate may be revoked by the Commission at any time upon service of a Notice of Revocation to the PIC or PIP.

SECTION 14. *Verification.* The Commission may, at any time, verify any or all registration information provided by a PIC or PIP through on-site examination of its data processing systems. Policies and documents identified in the registration, including proof of certifications attained, shall be made available to the Commission upon request.

SECTION 15. *Amendments or Updates.* Amendments or updates to registration information, including significant changes in the description of registered data processing systems, shall be made within two (2) months from the date such changes take into effect. For this purpose, a significant change shall include:

- A. name and contact details of the PIC or PIP, head of agency or organization, and DPO;
- B. a new or additional data processing system;
- C. an amendment or update to the description of a registered data processing system, particularly:
 - 1.) purpose or purposes of processing;
 - 2.) description of the category or categories of data subjects, and of their personal data or categories thereof;
 - 3.) recipients or categories of recipients to whom the personal data might be disclosed;
- D. a new or additional automated decision-making process;

Amendments or updates to the registration information may be undertaken through the online registration platform, subject to the approval of the Commission: *Provided*, that where the change consists of the appointment or designation of a new DPO, the submission of the appropriate supporting document must be undertaken.

SECTION 16. *Non-Registration.* A PIC or PIP shall be considered as unregistered under the following circumstances:

- A. failure to register with the Commission;
- B. expiration and non-renewal of certificate of registration;
- C. rejection or disapproval of an application for registration, or an application for renewal of registration; or
- D. revocation of the certificate of registration.

SECTION 17. *Renewal.* A PIC or PIP may file an application for the renewal of its certificate of registration within two (2) months prior to, but not later than the 8th day of March every year. Any registration relative to which no application for renewal has been filed within the prescribed period is deemed revoked: *Provided*, that a PIC or PIP may be allowed to file an application for renewal beyond the prescribed period upon approval of the Commission, and only for good cause shown. For this purpose, the PIC or PIP shall notify the Commission of its intention to renew its registration and the reason for its delay.

SECTION 18. *Reasonable Fees.* To recover administrative costs, the Commission may require the payment of reasonable fees for registration, renewal, and other purposes in accordance with a schedule that shall be provided in a separate issuance.

**RULE III.
REGISTRY OF DATA PROCESSING SYSTEMS**

SECTION 19. *Maintenance of Registry.* The Commission shall maintain a registry of data processing systems in electronic format.

SECTION 20. *Public Access to Registry.* Any person may inspect the registry during regular office hours: *Provided*, that the Commission shall regulate such access to protect the legitimate interests of PICs and PIPs.

Subject to reasonable fees and regulations that may be prescribed by the Commission, any person may also secure a duly certified copy of any entry from the registry relating to a particular PIC or PIP.

SECTION 21. *Amendments to Registry.* Amendments or updates to the registry shall be made by the Commission every two (2) months, or as often as necessary, in order to incorporate changes to the registration information filed by PICs or PIPs.

SECTION 22. *Removal from Registry.* The registration information of a PIC or PIP may be removed by the Commission from the registry on any of the following grounds:

- A. Incomplete registration;
- B. Expiration and non-renewal of registration;
- C. Revocation of certificate of registration; or
- D. Expired and void registration.

SECTION 23. *Non-inclusion of Confidential Information.* Information classified by the Constitution or any statute as confidential shall not be included in the registry.

**RULE IV.
NOTIFICATIONS REGARDING
AUTOMATED DECISION-MAKING**

SECTION 24. *Notification of Automated Decision-Making.* A PIC or PIC that carries out any automated decision-making operation shall notify the Commission via the mandatory registration process.

SECTION 25. *When to Notify.* Notifications regarding automated decision-making shall be included in the registration information that will be provided by a PIC or PIP, as indicated in Section 11 of this Circular, or through amendments or updates to such registration information, as per Section 15 of this Circular, within the prescribed periods.

SECTION 26. *Availability of Additional Information.* Upon request by the Commission, a PIC or PIP shall make available additional information and supporting documents pertaining to its automated decision-making operation, including:

- A. consent forms or manner of obtaining consent;
- B. retention period for the data collected and processed;
- C. methods and logic utilized for automated processing; and
- D. possible decisions relating to the data subject based on the processed data, particularly if they would significantly affect his or her rights and freedoms.

**RULE V.
SANCTIONS AND PENALTIES**

SECTION 27. *Revocation of Certificate of Registration.* The Commission may revoke the registration of a PIC or PIP on any of the following grounds:

- A. failure to comply with any of the provisions of the DPA, its IRR, or any relevant issuances of the Commission;
- B. failure to comply with any order, conditions, or restrictions imposed by the Commission;
- C. loss of authority to operate or conduct business, due to the revocation of its license, permit, franchise, or any other similar requirement provided by law;

- D. cessation of operations or of personal data processing;
- E. lack of capacity to process personal data in accordance with the DPA; or
- F. issuance by the Commission of a temporary or permanent ban on data processing against the PIC or PIP: *Provided*, that in the case of a temporary ban, such prohibition is still in effect at the time of filing of the application for renewal of registration:

Provided, that, prior to revocation, the Commission shall give the PIC or PIP an opportunity to explain why its certificate of registration should not be revoked.

SECTION 28. *Notice of Revocation.* Where the registration of a PIC or PIP is revoked, the Commission shall issue a Notice of Revocation of Registration, which shall be served upon the PIC or PIP.

SECTION 29. *Penalties and Fines.* A PIC or PIP whose certificate of registration has been revoked or that is determined to have violated the registration requirements provided in this Circular may, upon notice and hearing, be subject to compliance and enforcement orders, cease and desist orders, temporary or permanent bans on the processing of personal data, or payment of fines in accordance with a schedule to be issued by the Commission. For this purpose, the registration requirements shall pertain to the provisions on mandatory registration, amendments and updates, and renewal of registration.

Under the voluntary registration system, failure to comply by a PIC or PIP with the requirements on amendments and renewal, shall render its certificate of registration void.

SECTION 30. *Cease and Desist Order.* When the Commission, upon notice and hearing, has determined that a PIC or PIP failed to disclose its automated decision-making operation through the appropriate notification processes set out in this Circular, it shall cause the service upon the PIC or PIP a Cease and Desist Order on the processing of personal data: *Provided*, that this is without prejudice to any other administrative, civil, or criminal penalties that the PIC or PIP may incur under the DPA and other applicable laws.

**RULE VI.
MISCELLANEOUS PROVISIONS**

SECTION 31. *Transitory Period.* Notwithstanding the deadline for registration provided in the IRR, all PICs and PIPs covered by this Circular shall complete Phase I of the registration process by 9 September 2017. Phase II of the registration may be completed until 8 March 2018.

SECTION 32. *Repealing Clause.* All other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 33. *Separability Clause.* If any portion or provision of this Circular is declared null and void or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 34. *Effectivity.* This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or two (2) newspapers of general circulation.

Approved:

[Sgd] RAYMUND E. LIBORO
Privacy Commissioner

[Sgd] IVY D. PATDU
Deputy Privacy Commissioner

[Sgd] DAMIAN DOMINGO O. MAPA
Deputy Privacy Commissioner