

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

NPC Circular 16-02

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; HEADS OF PRIVATE ENTITIES

SUBJECT : DATA SHARING AGREEMENTS INVOLVING 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, Section 20 of the Implementing Rules and Regulations of the Data Privacy Act of 2012 provides that further processing of personal data collected from a party other than the data subject shall be allowed under certain conditions;

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 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, 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 data sharing agreements involving government agencies.

SECTION 1. *General Principle.* To facilitate the performance of a public function or the provision of a public service, a government agency may share or transfer personal data under its control or custody to a third party through a data sharing agreement: *Provided*, that nothing in this Circular shall be construed as prohibiting or limiting the sharing or transfer of any personal data that is already authorized or required by law.

SECTION 2. *Scope.* The provisions of this Circular shall only apply to personal data under the control or custody of a government agency that is being shared with or transferred to a third party, for the purpose of performing a public function, or providing of a public service: *Provided*, that it shall also cover personal data under the control or custody of a private entity that is being shared with or transferred to a government agency: *Provided further*, that where the personal data is in the custody of a personal information processor, the sharing or transfer of personal data shall only be allowed if it is pursuant to the instructions of the personal information controller concerned.

Data sharing agreements exclusively between private entities, or those for purpose of research, shall be in accordance with the Implementing Rules and Regulations of the Data Privacy Act of 2012, or other issuances of the National Privacy Commission.

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

- A. "Act" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- B. "Commission" refers to the National Privacy Commission (NPC);
- C. "Data Protection Officer" refers to an individual designated by the head of agency, or the head of a private entity, to be accountable for the agency's or entity's compliance with the Act, its IRR, and other issuances of the Commission: *Provided*, that 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 data protection officer;
- D. "Data sharing" is the disclosure or transfer to a third party of personal data under the control or custody of a personal information controller: *Provided*, that a personal information processor may be allowed to make such disclosure or transfer if it is upon the instructions of the personal information controller concerned.

The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor;

- E. "Data Sharing Agreement" refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: *Provided*, that only personal information controllers shall be made parties to a data sharing agreement;
- F. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;
- G. "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;

- H. "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;
- I. "Head of agency" refers to: (1) the head of the government entity or body, for national government agencies, constitutional commissions or offices, or branches of the government; (2) the governing board or its duly authorized official for government owned and controlled corporations, government financial institutions, and state colleges and universities; (3) the local chief executive, for local government units;
- J. "Head of a private entity" refers to the head or decision-making body of a private entity;
- K. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;
- L. "Middleware" refers to any software or program that facilitates the exchange of data between two applications or programs that are either within the same environment, or are located in different hardware or network environments;
- M. "Personal data" refers to all types of personal information;
- N. "Personal information controller" 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;

For the purpose of this Circular, each party to a data sharing agreement shall be considered a personal information controller.

- O. "Personal information processor" refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject;
- P. "Private entity" 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.

SECTION 4. Consent. The personal information controller charged with the collection of personal data directly from the data subject, on its own or through a personal information processor, shall obtain the consent of the data subject prior to collection and processing, except where such consent is not required for the lawful processing of personal data, as provided by law.

The personal information controller may request an advisory opinion from the Commission in determining whether the data sharing requires consent from the data subject.

The data subject shall be provided with the following information prior to collection or before his or her personal data is shared:

- A. Identity of the personal information controllers or personal information processors that will be given access to the personal data;
- B. Purpose of data sharing;
- C. Categories of personal data concerned;
- D. Intended recipients or categories of recipients of the personal data;
- E. Existence of the rights of data subjects, including the right to access and correction, and the right to object; and
- F. Other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

SECTION 5. *Data Privacy Principles.* Data sharing shall adhere to the data privacy principles laid down in the Act, the IRR, this Circular, and all applicable issuances of the Commission.

SECTION 6. *Content of a Data Sharing Agreement.* A data sharing agreement shall be in writing and must comply with the following conditions:

- A. It shall specify, with due particularity, the purpose or purposes of the data sharing agreement, including the public function or public service the performance or provision of which the agreement is meant to facilitate: *Provided*, that if the purpose includes the grant of online access to personal data, or if access is open to the public or private entities, these shall also be clearly specified in the agreement.
- B. It shall identify all personal information controllers that are party to the agreement, and for every party, specify:
 - 1. the type of personal data to be shared under the agreement;
 - 2. any personal information processor that will have access to or process the personal data, including the types of processing it shall be allowed to perform;
 - 3. how the party may use or process the personal data, including, but not limited to, online access;
 - 4. the remedies available to a data subject, in case the processing of personal data violates his or her rights, and how these may be exercised;
 - 5. the designated data protection officer or compliance officer.
- C. It shall specify the term or duration of the agreement, which may be renewed on the ground that the purpose or purposes of such agreement continues to exist: *Provided*, that in no case shall such term or any subsequent extensions thereof exceed five (5) years, without prejudice to entering into a new data sharing agreement.
- D. It shall contain an overview of the operational details of the sharing or transfer of personal data under the agreement. Such overview must adequately explain to a data subject and the Commission the need for the agreement, and the procedure that the parties intend to observe in implementing the same.
- E. It shall include a general description of the security measures that will ensure the protection of the personal data of data subjects, including the policy for retention or disposal of records.
- F. It shall state how a copy of the agreement may be accessed by a data subject: *Provided*, that the government agency may redact or prevent the disclosure of any detail or information that could endanger its computer network or system, or expose to harm the integrity, availability or confidentiality of personal data under its control or

custody. Such information may include the program, middleware and encryption method in use, as provided in the next succeeding paragraph.

- G. If a personal information controller shall grant online access to personal data under its control or custody, it shall specify the following information:
 - 1. Justification for allowing online access;
 - 2. Parties that shall be granted online access;
 - 3. Types of personal data that shall be made accessible online;
 - 4. Estimated frequency and volume of the proposed access; and
 - 5. Program, middleware and encryption method that will be used.
- H. It shall specify the personal information controller responsible for addressing any information request, or any complaint filed by a data subject and/or any investigation by the Commission: *Provided*, that the Commission shall make the final determination as to which personal information controller is liable for any breach or violation of the Act, its IRR, or any applicable issuance of the Commission.
- I. It shall identify the method that shall be adopted for the secure return, destruction or disposal of the shared data and the timeline therefor.
- J. It shall specify any other terms or conditions that the parties may agree on.

SECTION 7. *Online Access.* Where a government agency grants online access to personal data under its control or custody, such access must be done via a secure encrypted link. The government agency concerned must deploy middleware that shall have full control over such online access.

SECTION 8. *Transfer of Personal Data.* Where a data sharing agreement involves the actual transfer of personal data or a copy thereof from one party to another, such transfer shall comply with the security requirements imposed by the Act, its IRR, and all applicable issuances of the Commission.

SECTION 9. *Responsibility of the Parties.* All parties to a data sharing agreement shall comply with the Act, its IRR, and all applicable issuances of the Commission, including putting in place adequate safeguards for data privacy and security. The designated data protection officer shall be accountable for ensuring such compliance.

In the case of a government agency, the head of agency shall be responsible for complying with the security requirements provided in the Act, its IRR and all applicable issuances of the Commission.

SECTION 10. *Accountability for Cross-border Transfer of Personal Data.* Each party to a data sharing agreement shall be responsible for any personal data under its control or custody, including those it has outsourced or subcontracted to a personal information processor. This extends to personal data it shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.

SECTION 11. *Prior Consultation.* Prior to the execution of a data sharing agreement, the parties thereto may consult with and invite comments thereon from:

- A. the Commission;

- B. any person or organization that the parties to the proposed data sharing agreement recognize as representing the interests of the classes of data subjects whose personal data will be shared under the proposed agreement; and
- C. any other person or organization whose view or opinion the parties to the proposed data sharing agreement deem necessary.

Failure to conduct prior consultation by the parties shall not invalidate a data sharing agreement: *Provided, however,* that in the event of a breach or a reported violation of the Act, its IRR, or any issuance by the Commission, the latter shall take into account the conduct of such consultation in evaluating the circumstances surrounding the violation.

SECTION 12. *Security of Personal Data.* Data sharing shall only be allowed where there are adequate safeguards for data privacy and security. The parties to a data sharing agreement shall use contractual or other reasonable means to ensure that personal data is covered by a consistent level of protection when it is shared or transferred.

SECTION 13. *Review by the Commission.* A data sharing agreement shall be subject to a review by the Commission, on its own initiative or upon a complaint by a data subject.

SECTION 14. *Mandatory Periodic Review.* The terms and conditions of a data sharing agreement shall be subject to a mandatory review by the parties thereto upon the expiration of its term, and any subsequent extensions thereof. The parties shall document and include in its records:

- A. reason for terminating the agreement or, in the alternative, for renewing its term; and
- B. in case of renewal, any changes made to the terms and conditions of the agreement.

SECTION 15. *Revisions and Amendments.* Revisions or amendments to a data sharing agreement while it is still in effect shall follow the same procedure observed in the creation of a new agreement.

SECTION 16. *Termination.* A data sharing agreement may be terminated:

- A. upon the expiration of its term, or any valid extension thereof;
- B. upon the agreement by all parties;
- C. upon a breach of its provisions by any of the parties; or
- D. where there is disagreement, upon a finding by the Commission that its continued operation is no longer necessary, or is contrary to public interest or public policy.

Nothing in this Section shall prevent the Commission from ordering *motu proprio* the termination of any data sharing agreement when a party is determined to have breached any of its provisions, or when the agreement is in violation of the Act, its IRR, or any applicable issuance by the Commission.

SECTION 17. *Return, Destruction, or Disposal of Transferred Personal Data.* Unless otherwise provided by the data sharing agreement, all personal data transferred to other parties by virtue of such agreement shall be returned, destroyed, or disposed of, upon the termination of the agreement.

SECTION 18. *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 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 19. *Transitory Period.* Upon the effectivity of this Circular, all existing data sharing arrangements shall be reviewed by the concerned parties to determine compliance with its provisions.

Where an existing data sharing arrangement is not covered by any written contract, joint issuance, or any similar document, the parties thereto shall execute or enter into the appropriate agreement pursuant to the provisions of this Circular.

Where an existing data sharing agreement is evidenced by a contract, joint issuance, or any similar document, but fails to comply with the provisions of this Circular, the parties thereto shall make the necessary revisions or amendments.

An existing data sharing agreement found to be compliant with this Circular, except for the requirements set out in Section 4 (Consent) hereof, shall be allowed to continue until the expiration of such agreement or within two (2) years from the effectivity of this Circular, whichever is earlier, subject to the immediately succeeding paragraph: *Provided*, that any renewal or extension of such agreement shall comply with all the provisions of this Circular.

In all cases, the personal information controller that collected the personal data directly from the data subjects shall, at the soonest practicable time, notify and provide the data subjects whose personal data were shared or transferred without their consent with all the information set out in Section 4 (Consent) of this Circular: *Provided*, that where individual notification is not possible or would require a disproportionate effort, the personal information controller may seek the approval of the Commission to use alternative means of notification: *Provided, further*, that the personal information controller shall establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the data sharing agreement.

If an existing data sharing arrangement is not for the purpose of performing a public function or providing a public service, the parties thereto shall immediately terminate the sharing or transfer of personal data. Any or all related contracts predicated on the existence of such arrangement shall likewise be terminated for being contrary to law.

SECTION 20. *Repealing Clause.* All other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 21. *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 22. *Effectivity.* This Circular 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