Republic of the Philippines
NATIONAL PRIVACY COMMISSION

# NPC Circular No. 2020-03

**DATE : 23 December 2020**

**SUBJECT : DATA SHARING AGREEMENTS**

**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 21(a) of the Data Privacy Act of 2012 states that a personal information controller is accountable for complying with the requirements of the law and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party;

**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.

**SECTION 1.** ***Scope***. — The provisions of this Circular apply to personal data under the control or custody of a personal information controller (PIC) that is being shared, disclosed, or transferred to another PIC. The Circular likewise applies to personal data that is consolidated by several PICs and shared or made available to each other and/or to one or more PICs.

It excludes arrangements between a PIC and a personal information processor (PIP).

**SECTION 2.** ***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, also known as the Data Privacy Act of 2012;

B. "Commission" or "NPC" refers to the National Privacy Commission;

C. "Compliance Check" refers to the systematic and impartial evaluation of a PIC or PIP, in whole or any part, process or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the Data Privacy Act and other issuances of the Commission. It is an examination, which includes Privacy Sweeps, Documents Submissions and On-Site Visits, intended to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls and review mechanisms intended to assure privacy and personal data protection in data processing systems.

D. "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent is evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

E. "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 a government agency or private entity may have more than one DPO;

F. "Data sharing" is the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller to one or more other personal information controller/s.

   In the case of a personal information processor, data sharing should only be allowed if it is carried out on behalf of and upon the instructions of the personal information controller it is engaged with via a subcontracting agreement. Otherwise, the sharing, transfer, or disclosure of personal data that is incidental to a subcontracting agreement between a personal information controller and a personal information processor should be excluded;

G. "Data Sharing Agreement" or "DSA" refers to a contract, joint issuance, or any similar document which sets out the obligations, responsibilities, and liabilities of the personal information controllers involved in the transfer of personal data between or among

them, including the implementation of adequate safeguards for data privacy and security, and upholding the rights of the data subjects: *provided*, that only personal information controllers should be made parties to a data sharing agreement;

H. "Data subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

I. "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;

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, state colleges and universities;

K. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173;

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 and sensitive personal information;

N. "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;

O. "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 processed, or the purpose or extent of its processing.

P. "Personal information processor" or "PIP" 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;

Q. "Private entity" refers to any natural or juridical person, or any other body that is not a unit of the Philippine government or any other foreign government entities, such as but not limited to, stock and non-stock corporations, foreign corporations, partnerships, cooperatives, sole proprietorships, or any other legal entity.

R. "Privileged information" refers to any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication;

S. "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 individual, 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 is 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.

T. "Subcontracting" refers to the outsourcing, assignment, or delegation of the processing of personal data by a personal information controller to a personal information processor. In this arrangement, the personal information controller retains control over the processing.

U. "Subcontracting Agreement" refers to a contract, agreement, or any similar document which sets out the obligations, responsibilities, and liabilities of the parties to a subcontracting arrangement. It shall contain mandatory stipulations prescribed by the IRR.

**SECTION 3.** ***General principles.*** **—** Data sharing arrangements are executed between or among PICs only, and are governed by the following principles:

A. Adherence to the data privacy principles of transparency, legitimate purpose, and proportionality;

B. Fulfilment of all applicable requirements prescribed by the Act, its IRR, and other issuances of the Commission;

C. Recognition of and upholding the rights of affected data subjects, unless otherwise provided by law;

D. Ensuring that the shared and collected data are accurate, complete, and where necessary for the declared, specified, and legitimate purpose, kept up to date; and

E. Implementation of reasonable and appropriate organizational, physical, and technical security measures intended for the protection of personal data against any accidental or unlawful destruction, alteration, and disclosure, as well as against any other unlawful processing.

**SECTION 4.** ***Parties.*** **—** Only PICs can be parties to data sharing arrangements. This is the

case even where the actual sharing will transpire between a PIC and a PIP acting on behalf of, or upon the instructions of, another PIC.

**SECTION 5.** ***Transparency.*** **—** Each affected data subject should be provided with the following information before personal data is shared or at the next practical opportunity, through an appropriate consent form or privacy notice, whichever is applicable or appropriate to the lawful basis relied upon:

A. Categories of recipients of the personal data: *provided*, that PICs shall provide a data subject with the identity of the recipients, upon request;

B. Purpose of data sharing and the objective/s it is meant to achieve;

C. Categories of personal data that will be shared;

D. Existence of the rights of data subjects; and

E. Other information that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved.

In cases where consent is not required, a privacy notice is sufficient. Where the PIC has already collected the personal data, it should provide the data subjects with the information above as soon as it decides that personal data will be shared or as soon as possible afterwards.

It is a good practice for PICs to review their privacy notice regularly to ensure that it continues to reflect accurately the data sharing arrangement they are engaged in.

**SECTION 6.** ***Authorized processing.*** **—** Data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the Act: *provided*, that nothing in this Circular shall be construed as prohibiting or limiting the sharing, disclosure, or transfer of personal data that is already authorized or required by law.

**SECTION 7.** ***Special cases.*** **—** Data sharing may also be allowed pursuant to Section 4 of the Act, which specifies the special cases wherein the law and the rules are not applicable, but such data sharing should only be to the minimum extent necessary to achieve the specific purpose, function, or activity, and subject to the requirements of applicable laws, regulations, or ethical standards.

**SECTION 8.** ***Data sharing agreement; key considerations.*** **—** Data sharing may be covered by a data sharing agreement (DSA) or a similar document containing the terms and conditions of the sharing arrangement, including obligations to protect the personal data shared, the responsibilities of the parties, mechanisms through which data subjects may exercise their rights, among others.

The execution of a DSA is a sound recourse and demonstrates accountable personal data processing, as well as good faith in complying with the requirements of the DPA, its IRR, and issuances of the NPC. The Commission shall take this into account in case a complaint is filed pertaining to such data sharing and/or in the course of any investigation relating thereto, as well as in the conduct of compliance checks.

**SECTION 9.** ***Contents of a Data Sharing Agreement***. **—** The following constitute the contents

of a DSA:

A. *Purpose and lawful basis*. It specifies the purpose/s of the data sharing and the appropriate lawful basis.

B. *Objectives*. It identifies the objective/s that the data sharing is meant to achieve.

C. *Parties*. It identifies all PICs that are party to the DSA and, for each party, specifies the following:

    1. Type of personal data it will share, if any;
    2. Whether the personal data processing will be outsourced, including the types of processing PIPs or service providers will be allowed to perform;
    3. Method to be used for the processing of personal data; and
    4. Designated data protection officer.

D. *Term*. It specifies the term or duration of the data sharing arrangement which will be based on the continued existence of the purpose/s of such arrangement. Perpetual data sharing or DSAs that have indeterminate terms are invalid. Parties are free to renew or extend a DSA upon its expiration. The DSA should be subject to the conduct of periodic reviews which should take into consideration the sufficiency of the safeguards implemented for data privacy and security.

E. *Operational details*. It provides an overview of the operational details of the data sharing, including the procedure the parties intend to observe in implementing the same. If the recipient will be allowed to disclose the shared data, or grant public access to the same, this must be established clearly in the DSA, including the following details:

    1. Justification for allowing such access;
    2. Parties that are granted access;
    3. Types of personal data that are made accessible; and
    4. Estimated frequency and volume of such access.

    Where disclosure or public access is facilitated by an online platform, the program, middleware, and encryption method that will be used should also be identified.

    Any other information that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved should also be provided.

F. *Security*. It includes a description of the reasonable and appropriate organizational, physical, and technical security measures that the parties intend to adopt to ensure the protection of the shared data. The parties should also establish a process for data breach management.

G. *Data subjects' rights*. It provides for mechanisms that allow affected data subjects to exercise their rights relative to their personal data, including:

    1. Identity of the party or parties responsible for addressing: information requests, complaints by a data subject, and/or any investigation by the NPC: *provided*, that

the NPC shall make the final determination as to which party is liable for any violation of the Act, its IRR, or any applicable NPC issuance; and

2. Procedure by which a data subject can access or obtain a copy of the DSA: *provided*, that the parties may redact or prevent the disclosure of trade or industrial secrets, confidential and proprietary business information, and any other detail or information that could endanger or compromise their information systems, or expose to harm the confidentiality, integrity, or availability of personal data under their control or custody.

H. *Retention and Data Disposal*. It includes rules for the retention of shared data and identify the method that will be adopted for the secure return, destruction, or disposal of the shared data and the timeline therefor.

The parties may specify any other stipulations, clauses, terms and conditions as they may deem appropriate: *provided*, that they are not contrary to law, morals, public order, or public policy.

**SECTION 10.** ***Record of data sharing arrangements.*** – Each PIC should establish and maintain a record of its data sharing arrangements, including the following:

A. Contact details of all parties, including their respective data protection officers;

B. Legal bases for the data sharing arrangement/s;

C. Copy of the DSA/s, if executed;

D. Written, recorded, or electronic proof of the consent obtained from data subjects, where applicable; and

E. Date and/or time consent was obtained and withdrawn, where applicable.

Such record will allow the effective management of the PIC's third-party engagements. It should be kept accurate and up to date to allow the PIC to address any related inquiries and to demonstrate its compliance with the DPA.

**SECTION 11.** ***Security of shared personal data.*** – Adequate safeguards to protect personal data should be put in place in every data sharing arrangement, subject to the conditions set forth under Section 9 above.

Where online access to personal data is granted, the parties should ensure that said access is secure through the use of any appropriate program, software, or any other appropriate means, such as the use of a secure encrypted link or a middleware.

**SECTION 12.** ***Accountability.*** – All parties to a data sharing arrangement should comply with the Act, its IRR, this Circular, and all applicable issuances of the Commission. Subject to the terms of the DSA, each party will be responsible for any personal data under its control or custody, including those where the processing has been outsourced or subcontracted to a PIP. This extends to personal data each party shares with or transfers to a third party located outside the Philippines, subject to cross-border arrangement and cooperation.

The DPOs of the parties will sign as witnesses to the DSA.

**SECTION 13.** ***Review by the Commission***. — Data sharing, whether or not covered by a DSA, may be subject to review by the Commission, on its own initiative or upon a verified complaint by an affected data subject.

**SECTION 14.** ***Periodic review***. — Parties to data sharing, whether or not covered by a DSA, should subject the same to periodic reviews to determine the propriety of continuing the data sharing, taking into account the sufficiency of the safeguards implemented for data protection and any data breach or security incident that may have occurred affecting the shared data.

The terms and conditions of a DSA may be subject to review by the parties thereto upon the expiration of its term, and any subsequent extensions thereof. In reviewing the DSA, the parties should document and include in its records:

A. the 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***. — Changes to DSAs while it is still in effect should follow the same procedure observed in the creation of a new agreement.

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

A. upon the expiration of its term, or any valid extension thereof;

B. upon the agreement by all parties;

C. upon breach of any provisions of the DSA by any of the parties;

D. upon dissolution or death of the PIC;

E. upon a finding by the Commission that data sharing is:

    1. no longer necessary for the specified purpose/s and its objective/s has already been achieved; or
    2. detrimental to national security, public interest or public policy, or the termination of the same is necessary to preserve and protect the rights of a data subject.

Nothing in this Section prevents the Commission from ordering *motu proprio* the termination of any data sharing, whether or not covered by a DSA, when a party is determined to have violated 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 DSA, all personal data transferred to other parties by virtue of a data sharing, whether or not covered by a DSA, should be returned, destroyed, or disposed of, upon the termination of the arrangement.

**SECTION 18.** ***Transitory period.*** — Where an existing data sharing is not covered by any written contract, joint issuance, or any similar document, the parties thereto may execute or enter into an appropriate agreement, subject to the considerations set forth under Section 8 of

this Circular.

All existing DSAs should be reviewed by the concerned parties to determine compliance with the provisions of this Circular and make the necessary revisions or amendments, as may be appropriate.

In all cases, the PIC that collected the personal data directly from the data subjects should, at the soonest practicable time, notify and provide the data subjects whose personal data were shared, transferred, or disclosed with all the information set out in Section 5 of this Circular: *provided*, that where individual notification is not possible or would require a disproportionate effort, the PIC may seek the approval of the Commission to use alternative means of notification: *provided further*, that the PIC should establish means through which the data subjects can exercise their rights and obtain more detailed information relating to the DSA.

**SECTION 19.** ***Separability Clause***. **—** If any portion or provision of this Circular is declared invalid or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

**SECTION 20.** ***Repealing Clause***. **—** This Circular supersedes in its entirety NPC Circular No. 16-02. The provisions of the IRR and all other issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

**SECTION 21.** ***Effectivity***. **—** This Circular takes effect fifteen (15) days after its publication in the Official Gazette or two newspapers of general circulation.

Approved:

**SGD.**
**RAYMUND ENRIQUEZ LIBORO**
Privacy Commissioner

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

**SGD.**
**JOHN HENRY D. NAGA**
Deputy Privacy Commissioner