Title:

Ensuring Privacy and Accountability in Data Sharing

Brief Overview:

The article explains how data sharing in the Philippines is regulated under the Data Privacy Act of 2012. It emphasizes the necessity of certain security safeguards and requirements to protect data subjects' rights and ensure compliance.

Full Article:

In the Philippines, the practice of data sharing is regulated by the National Privacy Commission ("NPC") through the implementation and administration of Republic Act No. 10173, also known as the Data Privacy Act of 2012 ("DPA"). The DPA was enacted to protect the fundamental human right to privacy while at the same time ensuring the free flow of information necessary for innovation and economic growth. Within this legal framework, data sharing is not prohibited but is subject to strict rules and safeguards designed to protect individuals whose personal data is involved.

Data sharing is defined as the sharing, disclosure, or transfer to a third party of personal data under the custody of a personal information controller ("PIC") to one or more other PIC/s. In the case of a Personal Information Processor ("PIP"), 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.[1] Data sharing arrangements are executed between or among PICs only.[2]

Data sharing shall be considered lawful only when it complies with the conditions set out in the DPA, particularly, the following:[3]

1. When it is expressly authorized by law: Provided, that there are adequate safeguards for data privacy and security, and processing adheres to principle of transparency, legitimate purpose and proportionality;

2. In the private sector, when the data subject[4] consents to data sharing, and the following conditions are complied with:

    a. Consent for data sharing shall be required even when the data is to be shared with an affiliate or mother company, or similar relationships; and

[1] Rule I, Section 3, Implementing Rules and Regulations of Republic Act No. 10173, also known as the "Data Privacy Act of 2012" ("DPA IRR").
[2] Section 3, NPC Circular No. 2020-03.
[3] Rule II, Section 20, DPA IRR.
[4] Data subject refers to the individual whose personal, sensitive personal, or privileged information is processed.

b. Data sharing for commercial purposes, including direct marketing, shall be covered by a data sharing agreement which shall establish adequate safeguards for data privacy and security, uphold the rights of data subjects, and be subject to review by the Commission, on its own initiative or upon complaint of a data subject.

3. When the data subject is provided with the following information prior to collection or before 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; f) other information that would sufficiently notify the data.

Pertinent to data sharing in the context of economic growth is the sharing of data for commercial purposes, which requires the execution of a data sharing agreement ("DSA").

A DSA refers to a contract, joint issuance, or any similar document that 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. To note, only PICs can be parties to a DSA.[5] This rule shall be applicable even when the actual sharing will transpire between a PIC and a PIP acting on behalf of, or upon the instructions of, another PIC.[6]

The NPC, through NPC Circular No. 2020-03, provided the minimum contents of a DSA, *to wit:*[7]

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

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

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

    a. Type of personal data it will share, if any;
    b. Whether the personal data processing will be outsourced, including the types of processing that PIPs or service providers will be allowed to perform;
    c. Method to be used for the processing of personal data; and

[5] Section 2(G), NPC Circular No. 2020-03.
[6] Section 4, NPC Circular No. 2020-03.
[7] Section 9, NPC Circular No. 2020-03.

d. Designated data protection officer.

4. 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.

5. 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:

    a. Justification for allowing such access;
    b. Parties that are granted access;
    c. Types of personal data that are made accessible; and
    d. 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.

6. 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.

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

    a. 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
    b. 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.

8. Retention and Data Disposal. It includes rules for the retention of shared data and identifies the method that will be adopted for the secure return, destruction, or disposal of the shared data and the timeline therefore.

Further, in NPC Advisory No. 2025-01, the NPC clarified that its pre- or post-execution review and approval of DSAs is not required. However, it clarified that it may review the data sharing activity itself, whether or not covered by DSAs, on its own initiative or upon a verified complaint by an affected data subject.[8]

In sum, data sharing under the DPA is not inherently prohibited, but it is strictly regulated to protect individuals' privacy rights while supporting legitimate economic and social activities. Commercial data sharing, in particular, must be conducted through a well-defined Data Sharing Agreement between PICs, ensuring that the purpose, security safeguards, operational procedures, and data subject rights are clearly articulated and upheld. Although prior NPC approval of DSAs is not required, the NPC retains the authority to review any data sharing activity, underscoring the importance of compliance, accountability, and transparency in the responsible exchange of personal data.

Authors:

Enrique V. Dela Cruz, Jr.
Senior Partner, DivinaLaw
enrique.delacruz@divinalaw.com

Janna Mae B. Tecson
Partner, DivinaLaw
janna.tecson@divinalaw.com

Kristina Mae C. Durana
Senior Associate, DivinaLaw
kristina.durana@divinalaw.com

Clarizza Grace D. Napa
Associate, DivinaLaw
clarizza.napa@divinalaw.com

[8] Section 1(E), NPC Advisory No. 2025-01.