Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2017-28

23 June 2017

[redacted]

Re: DATA SHARING AGREEMENT BETWEEN GOVERNMENT AGENCIES

Dear [redacted]

This is with regard to your queries received by the National Privacy Commission (NPC) on 4 April 2017 with regard to data sharing between government agencies, to wit:

1. Can data be shared between government agencies even in the absence of a law (IRR, Sec. 20, a.) or consent (IRR, Sec. 20, c.) as long as there is a data sharing agreement? Stated another way, if there is a data sharing agreement between two (or more) government agencies, does that dispense with the requirement for a law authorizing the sharing or consent?

2. Section 20(a) states that data sharing shall only be allowed when it is expressly authorized by law. What law falls within this context? Should it be interpreted strictly as a law equal in standing to the Data Privacy Act (Republic Act)? Or would a looser interpretation of "law" suffice? For example, does it make any difference if an issuance authorizing data sharing is an Executive Order? Administrative Order? Memorandum Circular? Department Order? Ordinance? For that matter, would internal office issuances/policies suffice? If, for example, the head of an agency issues an appropriate issuance (order, circular, etc.) directing that data be shared, does that satisfy the requirement for an "authorization by law"?

3. Can a data subject provide informed consent if he or she is not provided specific information regarding the purposes for which his or her data is to be used, for example if data is to be mined for general purposes in a data warehouse? (Section 19(a)(2)) Under said circumstances, can the data still be shared?

Data sharing between government agencies

Section 20 of the Implementing Rules and Regulation (IRR) of the Data Privacy Act of 2012 (DPA) provides for the general requirements when data sharing is allowed, i.e., when it is expressly authorized by law and provided that there are adequate safeguards for data privacy and security, and that processing adheres to principle of transparency, legitimate purpose, and proportionality.[1]

Particularly for data sharing between government agencies, Section 20(d) of the IRR applies. It states that:

> "d. Data sharing between government agencies for the purpose of a public function or provision of a public service shall be covered by a data sharing agreement.
>
> 1. Any or all government agencies party to the agreement shall comply with the Act, these Rules, and all other issuances of the Commission, including putting in place adequate safeguards for data privacy and security.
> 2. The data sharing agreement shall be subject to review of the Commission, on its own initiative or upon complaint of data subject." (Underscoring supplied)

The Commission has also issued NPC Circular 16-02 which sets out guidelines for data sharing agreements involving government agencies. Section 1 of the Circular provides:

> "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."

Further, Section 19 of the said circular provides that "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."

[1] See: IRR of RA No. 10173, §20(a)

From the foregoing, it is clear that the data sharing of government agencies should always have a basis in law in order to fulfill the performance of a public function and provision of a public service.

As to consent, generally, the personal information controller charged with the collection of personal data from the data subject shall obtain the consent of the data subject prior to collection and processing.[2] This rule does not apply where such consent is not required for the lawful processing of personal data, as provided by law.[3]

Thus, there should always be a basis in law which mandates the sharing of information for a public function or service. This requirement may not be dispensed with by the mere fact that government agencies have executed data sharing agreements amongst themselves.

"Law" in the context of the DPA

Law, in the context of the DPA, is understood in its generic sense. It would include statutes enacted by the legislature, presidential issuances such as executive orders, administrative orders, rules and regulations promulgated by administrative bodies by virtue of its rule-making authority, ordinances passed by the *Sanggunian* of local government units, and rules promulgated by the Supreme Court pursuant to its rule-making power.

With regard to issuances and/or policies issued by the head of an agency, administrative regulations enacted by administrative agencies to implement and interpret the law which they are entrusted to enforce have the force of law and are entitled to respect. Such rules and regulations partake of the nature of a statute and are just as binding as if they have been written in the statute itself.[4]

Informed consent and personal data in a data warehouse

The DPA defines consent as any freely given, specific, informed indication of will whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her.[5] The law also provides for the right of the data subject to be informed whether personal information about him or her are being or have been processed. Further, he or she also has the right to be furnished information regarding the collection and processing such as description of the personal information to be entered into the system, the purposes for which they are being or are to be processed, and the recipients to whom they may be disclosed.[6]

---

[2] NPC Circular No. 16-03, §4
[3] Id.
[4] ABAKADA Guro Party List vs. Purisima, G.R. No. 166715, August 14, 2008.
[5] RA No. 10173, §3(b)
[6] See: RA No. 10173, §16(a) and (b)

Considering these provisions, it cannot be said that a data subject is giving an informed consent when he or she is not provided with pertinent information regarding the collection and processing of his or her personal information.

However, with regard to personal data mined for general purposes in a data warehouse, it is possible that the personal data may still be subject of data sharing even without consent of data subject as the processing may fall under any of the listed criteria for lawful processing specified in Sections 12 and 13 of the DPA. Personal data collected for other purposes may also be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods provided that adequate safeguards are guaranteed by said laws authorizing their processing.

For your reference.

Very truly yours,

IVY GRACE T. VILLASOTO
Chief
Policy Development Division