Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2022-006[1]

28 February 2022

[redacted]

RE: REQUEST FOR CUSTOMER'S PERSONAL DATA AND TRANSACTION HISTORY WITH A PRIVATE COURIER

Dear [redacted],

We write in response to your request for an Advisory Opinion received by the National Privacy Commission (NPC) on whether to grant the request of the Philippine Drug Enforcement Agency (PDEA) for certain personal data including the transaction history of one of your clients.

We understand that your company is engaged in logistics delivery and e-commerce business, acting as courier of parcels of your customers for delivery to their own clients. Thus, the company processes personal information of its customers as well as the latter's clients.

We understand further that the PDEA request was made pursuant to an ongoing investigation of the individual named in the request for illegal drug trafficking by means of courier platforms.

Further, we understand that there is an existing Memorandum of Agreement (MOA) between your company and the PDEA on coordination and mutual assistance for the effective and efficient implementation of the Comprehensive Dangerous Drugs Act of 2002,[2] with provisions on the duties and obligations of the parties, which includes assistance in the collection, processing, and analysis of information on illegal drug activities. The pertinent provisions included in your letter reads, *viz:*

a. Assist the PDEA in collecting, processing, and analyzing information on illegal drug

[1] Tags: special cases; public authority; law enforcement; constitutional and statutory mandate; proportionality.
[2] An Act Instituting The Comprehensive Dangerous Drugs Act Of 2002, Repealing Republic Act No. 6425, Otherwise Known As The Dangerous Drugs Act Of 1972, As Amended, Providing Funds Therefor, And For Other Purposes [Comprehensive Dangerous Drugs Act of 2002], Republic Act No. 9165 (2002)

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL https //www privacy gov ph/ Email Add info@privacy gov ph * Tel No 8234-2228

activities by promptly notifying it within (24) (sic) hours;

b. Assist PDEA in gathering information, monitoring, and identification of suspected drug trafficking activities;
c. Relay, deliver and report timely intelligence information or all other information obtained in the course of their business shall be brought to the PDEA for the purpose of anti-drug operations;

x x x

m. To grant access to the authorized members of the PDEA, to the merchandise/items being sold, or about to be transported from the seller and/or from their facility/warehouse to the prospective buyer/client, whenever there is an intelligence report of merchandise, item or good suspected to be containing dangerous drugs and controlled precursors and essential chemicals."

You mentioned that your company is inclined to deny the request in view of the prohibitions of the Data Privacy Act of 2012[3] (DPA) but noted the exceptions under Section 4 (e) of the law pertaining to information necessary in order to carry out the functions of public authorities. You now ask whether your company may grant the PDEA's request.

Scope of the DPA; special cases under the DPA; public authority; mandate; law enforcement

The DPA and its Implementing Rules and Regulations[4] (IRR) provide for a list of specified information which do not fall within the scope of the law.[5] In particular, information necessary to carry out the functions of a public authority are considered special cases under the IRR, *to wit:*

> "SECTION 5. Special Cases. The Act and these Rules shall not apply to the following specified information, only to the minimum extent of collection, access, used, disclosure or other processing necessary to the purpose, function, or authority concerned: x x x
>
> d. Information necessary in order to carry out the functions of public authority, in accordance with a constitutionally or statutorily mandated function pertaining to law enforcement or regulatory function, including the performance of the functions of the independent, central monetary authority, subject to restriction provided by law. Nothing in this Act shall be construed as having amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
>
> x x x
>
> *Provided,* that the non-applicability if the Act or these Rules do not extend to personal information controllers or personal information processors who remain subject to the requirements of implementing security measures for personal data protection: Provided further, that the processing of the information provided in the preceding paragraphs shall be exempted from the requirements of the Act only to the minimum extent

[3] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).
[4] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173 (2016).
[5] *Id.* § 4 (e) (2012).

necessary to achieve the specific purpose, function or activity."[6] (Underscoring supplied)

The above special case provides for qualifications or limitations on the application of the provisions of the DPA and its IRR. This means that when the personal and/or sensitive personal information (collectively, personal data) is needed to be processed by a public authority, such as the PDEA, pursuant to its statutory mandate, the processing of such personal data may be allowed under the law, to the minimum extent of collection, access, use, disclosure, or other processing necessary to the purpose, function, or activity concerned.

The following should guide the company in relation to the above-quoted provision:

a) The information is necessary in order to carry out the law enforcement functions. Where the processing activity violates the Constitution, or any other applicable law, the processing will not be considered necessary for law enforcement purposes;
b) The processing is for the fulfillment of a constitutional or statutory mandate; and
c) There is strict adherence to all due process requirements. Where there is a nonconformity with such processes, such processing shall not be deemed to be for a special case.[7]

Please also note that the interpretation of the aforementioned provision shall be strictly construed - only the specified information is outside the scope of the DPA, and the public authority remains subject to its obligations as a personal information controller (PIC) under the DPA such as implementing security measures to protect personal data, upholding the rights of data subjects, and adhering to data privacy principles, among others.[8]

We further note that the PDEA is created under the Comprehensive Dangerous Drugs Act of 2002. Under the law, one of PDEA's powers and duties is the initiation of investigative operations related to drug related activities, to wit:

> "(b) Undertake the enforcement of the provisions of Article II of this Act relative to the unlawful acts and penalties involving any dangerous drug and/or controlled precursor and essential chemical and investigate all violators and other matters involved in the commission of any crime relative to the use, abuse or trafficking of any dangerous drug and/or controlled precursor and essential chemical x x x" (Underscoring supplied)

Thus, PDEA's request for personal data and transaction history of your identified client may fall under the processing of personal data under a special case as discussed above vis-à-vis its mandate.

Data sharing; data sharing agreements

A data sharing agreement (DSA) refers to a contract, joint issuance or any similar document which sets out the obligations, responsibilities, and liabilities of the PICs involved in the transfer of personal data between or among them, including the implementation of adequate standards for data privacy and security and upholding rights of data subject.

We note that the MOA you executed with PDEA may be considered as a form of DSA as

[6] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 5 (d) (2016).
[7] *See:* National Privacy Commission, NPC Advisory Opinion No. 2021-018 (18 June 2021).
[8] See: National Privacy Commission, NPC Advisory Opinion Nos. 2020-015 (24 Feb 2020) and 2021-028 (16 July 2021).

majority of its provisions deal with further processing of personal data in your possession.

Indeed, although the execution of a DSA is not mandatory, it is still considered as a best practice as provided under NPC Circular No. 2020-03[9], to wit:

> "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 agreement, including obligations to protect the personal data shared, the responsibilities of the parties, mechanism 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 to, as well as in the conduct of compliance checks."

It is also important to note that data sharing may be based on any of the criteria for lawful processing of personal data in Sections 12 and 13 of the DPA and also in pursuant to Section 4 of the law which enumerates the special cases.

As discussed above, although DSAs are not mandatory, the execution of such agreement is encouraged as the same demonstrates accountability of the involved PICs.

General data privacy principles; proportionality

However, we emphasize that while there may be a legal ground in the granting of the request, the same shall only be to the minimum extent and in proportion to the purpose declared in their request, in keeping with the general data privacy principle of proportionality.

Thus, the disclosure should be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. These qualifiers serve as the measures by which a determination can be made on whether processing is proportional and justified in relation to the declared purpose. Further, this principle requires that personal data shall only be processed if the purpose of the processing could not reasonably be fulfilled by other means.

Therefore, indiscriminate disclosure of all personal data in your possession might not be the best recourse as this could be a violation of the principle of proportionality.

For this purpose, the company should check the different categories of personal data that it processes to have an initial determination of whether the disclosure thereof is relevant to the PDEA's investigation based on the information in the letter request as well as the other discussions between the company and PDEA. Alternatively, the company may disclose to PDEA the categories of personal data that it has and ask PDEA for feedback on the particulars of what they need and how the same relates to the investigation.

Finally, please note that the discussions above pertain to the processing of personal data as provided for under the DPA, its IRR, and issuances of the NPC and do not encompass the

[9] National Privacy Commission, Data Sharing Agreements [NPC Circular No. 2020-03] (23 December 2020).

appropriate requirements for the validity of a search and/or seizure of the contents of the parcel/s of your clients.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) IVY GRACE T. VILLASOTO
OIC-Director IV, Privacy Policy Office

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL https //www privacy gov ph/ Email Add info@privacy gov ph * Tel No 8234-2228