PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2023-017[1]

28 September 2023

[redacted]

RE: REQUEST OF GOVERNMENT AGENCIES TO ACCESS PNP'S CRIME INFORMATION, REPORTING AND ANALYSIS SYSTEM (CIRAS) AND OTHER DATABASES.

Dear [redacted]:

This refers to the request of the Directorate for Investigation and Detective Management for an Advisory Opinion on the data privacy implications of the request of some government agencies to access the Philippine National Police's (PNP) Crime Information, Reporting and Analysis System (CIRAS) and other databases.

We understand that CIRAS is a web-based database of the PNP that stores the data of all criminal complaints and reports, as well as the information of the victims and suspects. It includes the narrative reports contained in police blotters nationwide.

We gather that some government agencies have requested the PNP to have direct access to the CIRAS but without stating the purpose thereof. Thus, you seek guidance on whether it is permissible to grant the request considering that it stores both personal information and sensitive personal information.

Criminal records containing personal data.

The Data Privacy Act of 2012 (DPA) protects individual personal information in information and communications systems in the government and the private sector.[2] 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. On the other hand, the DPA classifies the following as sensitive personal information, *viz.:*

[1] Lawful Processing; Contractual Obligation; Legitimate Interest; Accountability.
[2] 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).

x x x

> *(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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;***[3] *(Emphasis Supplied)*

x x x

Applying the foregoing to your present concern, since the CIRAS contains data of criminal complaints and reports including information pertaining to victims and suspects, its contents are considered as sensitive personal information under the DPA. As a general rule, the processing of sensitive personal information is prohibited. Nevertheless, Section 13 of the DPA provides for instances where processing of sensitive personal information may be allowed, such as when:

> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, **or when provided by government or public authority**. (Emphasis supplied)

Thus, granting government agencies access to the CIRAS database is considered lawful processing of sensitive personal information as the information shall be provided to the government or public authority.

Furthermore, Section 4 of the DPA also recognizes special cases where the DPA's application may be limited or qualified, thus:

> (e) **Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.** Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA);
>
> (Emphasis supplied)

To assist you in evaluating a request for access by a government agency, it is worth revisiting the relevant discussions in NPC Advisory Opinion No. 2022-06[4] thus:

> 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

[3] *Ibid*, § 3 (g), (l).

[4] National Privacy Commission, NPC Advisory Opinion No. 2022-06 (28 February 2022).

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 should not be deemed to be a special case.

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.

(Emphasis Supplied)

As such, there is a basis under the DPA for the PNP to allow other government agencies to access the CIRAS as discussed above. However, each request must still be evaluated taking into account the attendant circumstances of the request for access, the type of personal data sought, and the mandate of the government agency involved.

General data protection principles; proportionality.

Please note that even if there is a legal basis for processing, the DPA does not permit unbridled processing of personal data. Personal Information Controllers (PICs), as the PNP in this case, are still required to adhere to the general data privacy principles set forth under the law.

One such principle is the principle of proportionality which states that the processing of personal data shall be adequate, relevant, suitable necessary and not excessive in relation to a declared specified purpose. It also states that personal data shall only be processed only if the purpose of the processing could not be reasonably fulfilled by any other means.[5] Thus, disclosure of personal data to requesting entities should be limited to its declared, specified, and legitimate purpose. In addition, only those personal data that are needed in relation to the declared and stated purpose should be disclosed to the requesting entities, which may be determined by the PNP on a case-to-case basis.

In NPC Advisory Opinion No. 2020-036,[6] we discussed the matter of inter-agency requests between PICs and its relation to the data privacy principle of proportionality, *viz.:*

[5] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, §18 (c) (2016).
[6] National Privacy Commission, NPC Advisory Opinion No. 2020-36 (8 September 2020)

While the requested documents, such as the certificates of title and tax declarations, are the best proof of ownership and sufficient basis for inferring possession over a parcel of land, respectively, which means that the said documents shall significantly facilitate the identification of the current owners and possessors of the affected properties, **there is a need to evaluate whether releasing actual copies of the same is proportional to the purpose of identification of owners/possessors.**
NGCP should consider whether it may be reasonable and acceptable for the respective Register of Deeds, the Assessors' Offices and the city or municipal planning offices of the affected LGUs **to provide certifications/lists of names and contact details of the owners/possessors per official records instead, without necessarily releasing copies of the land documents.**

This is in adherence to the *principle of proportionality* which requires that the processing, which includes disclosure, of personal information must be limited only to the extent that it is necessary to achieve the stated purpose and that there are no other effective means to achieve the same.

Nevertheless, we wish to emphasize that access to copies of the requested land documents may only be **allowed if NGCP has duly justified and substantiated its lawful interest over the subject properties and that denial of said request shall cause NGCP's failure to comply with its legal obligations under its franchise with the Philippine government. Such determination and assessment should be duly documented. And in this scenario, the respective Registry of Deeds, the Assessors' Offices and the city or municipal planning offices may provide the requested documents to NGCP, relying on such evaluation vis-à-vis the NGCP's mandate.**

We further reiterate that **compliance with legal obligations and with provisions of other existing laws and regulations, as well as processing of sensitive personal information for the establishment or exercise of legal claims may be validly done and are not necessarily violations of the DPA**. The provisions of applicable laws and regulations should be read together and harmonized with the DPA.

(Emphasis Supplied)

Thus, in keeping with the data privacy principles, particularly on proportionality, any request for access to the CIRAS database containing personal data should undergo evaluation and judicious assessment to determine what specific personal data should be disclosed, and if the request is proportional to the purpose sought by the requesting agency.

Data Subject Rights; safeguards; penalties under the DPA

Under the DPA, PICs are required to implement organizational, physical, and technical security measures in their processing of personal data. It is imperative that guidelines must be crafted on the grant of access to other government agencies in your organization's Privacy Manual or Manual of Operations. This is to ensure that data subjects' personal data is kept secure and protected. Further, mechanisms should be put in place where data subjects may exercise their rights under the DPA, when appropriate and applicable.

Finally, we emphasize that the DPA is not intended to hamper or interfere with the performance of duties and functions of duly constituted public authorities. The DPA does not prohibit government agencies from processing personal data pursuant to their respective mandates, taking into consideration the applicable provisions of law, rules and regulations, and the general data privacy principles enunciated in the DPA.

Please be advised that this Advisory Opinion was rendered based solely on the information you have provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN, IV
Director IV, Privacy Policy Office