



22 August 2019

### **ADVISORY OPINION**

Reference No. DPO 19-37

FOR : [REDACTED]

CC: [REDACTED]  
[REDACTED]

SUBJECT : **PNP Request for Certification and Records**

Dear [REDACTED]:

We address your data privacy concerns regarding the request of the Philippine National Police (PNP) for information on an alleged former member of the [REDACTED] of UP Diliman.

### **Facts**

- On 05 August 2019, the [REDACTED] received a letter from [REDACTED] of the Major Crimes Investigation Unit of the Criminal Investigation and Detection Group (CIDG) of the PNP.
- The letter requests for information on “[REDACTED], a former [REDACTED] and [REDACTED] of [REDACTED], UP Diliman [REDACTED]”.
- The letter requests for “a copy of certification whether the aboved name person have connection in your University or any records pertaining to this individual”.
- On 19 August 2019, through a series of referrals for appropriate action, the UP Diliman Data Protection Officer received the [REDACTED]’s request for data privacy guidance.

### **Issue**

- Can UP Diliman legal provide the information requested by PNP?

### Advisory Opinion

**No, the request cannot be granted in the absence of a search warrant.** The 1987 Constitution guarantees the right against warrantless searches and seizures.

The requested educational information are *sensitive* personal information, the disclosure of which is prohibited by law save for limited exceptions. Although *providing* information to a public authority is among the exceptions, PNP's act of *collecting* information is not. PNP must still comply with the requirements of having a search warrant and non-excessive collection of personal information.

The request cannot be granted for being broad, sweeping, and excessive:

- (1) Requesting for the individual's "connection" and "any records" with UP is broad because it does not describe the specific information sought to be obtained. Granting it would unduly allow a "fishing expedition" for evidence;
- (2) The letter has a sweeping purpose because PNP did not declare the specifics how the requested certification and records will be used for a legitimate purpose; and
- (3) A "certification" is excessive because PNP already declared in its letter that the individual was "██████████" of UP. The request for "any records" is also excessive because the National Privacy Commission only allows collection of information "to the minimum extent necessary to achieve the specific purpose, function, or activity of the public authority."

To avoid any allegation from the PNP that UP is reasoning in favor of the individual, it is suggested that UP's reply be succinct. UP may simply state that while it supports the PNP in its endeavors, it unfortunately cannot grant the request as UP is constrained to comply with Article III Section 2 of the 1987 Constitution.

Any future disclosure of the individual's information must be communicated to the individual to afford him his "right to information".

## Discussion

### ***Necessity of a search warrant***

No less than the Bill of Rights of the 1987 Constitution establishes the fundamental right of the people to be secure in their papers and documents; it states:

“ARTICLE III

Bill of Rights

*x x x*

SECTION 2. The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.”

The arrival of the Data Privacy Act of 2012<sup>1</sup> did not repeal the people’s constitutional right to be secure in their papers and documents *unless there is a search warrant*.

In an analogous case where the National Bureau of Investigations (NBI) sent a letter to a school requesting for school records, the National Privacy Commission (NPC) stated that allowing a letter-request to substitute for a search warrant would grant NBI limitless power to gather information. The relevant NPC Advisory Opinion states:<sup>2</sup>

“The right against unreasonable searches and seizures guards against the exercise of government of unbridled discretion in collecting, obtaining and using information relevant to individuals, for whatever purpose. **The request for disclosure of ‘school records’** as in this case, *‘in connection with the investigation being conducted by this Bureau’* **is not the same as the issuance of a search warrant**. If it were so, then it would be akin to issuing a general search warrant through a mere letter-request, rendering the power of the NBI limitless to gather information, even in those cases where individuals have overriding privacy interests.”

[Emphases supplied]

In the absence of a search warrant, the PNP’s investigation cannot be allowed to an extent that it is already “overriding privacy interests.”

---

<sup>1</sup> Republic Act No. 10175.

<sup>2</sup> National Privacy Commission Advisory Opinion No. 2018-071, 05 October 2018.

To emphasize the need for full respect for privacy, the NPC further stressed:

“The DPA should always be interpreted in a manner consistent with the full respect for human rights enshrined in the Constitution.”

***Processing of sensitive personal information is prohibited by law. The request is not among the exceptions.***

A “certification” that a person was or was not accepted and enrolled in UP is educational information. PNP’s predicate relationship between UP and the concerned individual is an educational relationship. Hence, “any records” UP may have regarding the individual is also educational information.

Educational information is classified as *sensitive* personal information.<sup>3</sup> The processing<sup>4</sup> of sensitive personal information – *which includes disclosure* – is prohibited except for certain limited exceptions in the Data Privacy Act:

“SEC. 13. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information **shall be prohibited**, except in the following cases:

- (a) The data subject has given his or her consent *x x x*;
- (b) The processing is provided for by existing laws and regulations *x x x*;
- (c) The processing is necessary to protect the life and health of the data subject or another person *x x x*;
- (d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations *x x x*;
- (e) The processing is necessary for purposes of medical treatment *x x x*;  
or
- (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 to government or public authority.**”

[Emphases supplied]

The last listed exception is the one applicable to the matter at hand. Section 13(f) states that sensitive personal information may be processed “when provided to government or public authority.” The use of the term “provided” means that the exception only applies to the act of *providing* information to a public authority. However, the act of *collecting* information is still not

---

<sup>3</sup> Data Privacy Act of 2012, Section 3(l)(2).

<sup>4</sup> “Processing” includes collection and disclosure of information (see Data Privacy Act Section 3(j)). PNP is currently collecting information. UP should avoid disclosing information.

exempted because the collecting authority (in this case, the PNP) still has to comply with constitutional requirements (in this case, a search warrant) as well as statutory requirements (in this case, non-excessive processing as discussed below).

PNP's letter is also not a substitute to a subpoena under Republic Act No. 10973.<sup>5</sup>

***The request cannot be granted for being broad, sweeping, and excessive***

The request is broad.

Requesting for the individual's "connection" and "any records" with UP is a broad request. There is no description of the specific information sought to be obtained. If granted, this broad request will allow "a fishing expedition to confiscate any and all kinds of evidence or articles relating to a crime"<sup>6</sup> – an act which the PNP is prohibited to conduct.

The request has a sweeping purpose.

The purpose is "for allegedly violations of R.A. 11188, Article 271 of R.P.C., R.A. 7610 and R.A. 9851." This is a sweeping purpose which violates the privacy principle of *proportionality*<sup>7</sup> because the connection of the requested certification and records to PNP's purpose is *not specified*.

Only information compatible with a declared, specified and legitimate purpose may be collected. The law states:<sup>8</sup>

"SEC. 11. *General Data Privacy Principles.* –

*x x x*

Personal information must be:

- (a) **Collected for specified and legitimate purposes** determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such **declared, specified and legitimate purposes only;**"

---

<sup>5</sup> Republic Act No. 10973 grants the Chief of the Philippine National Police (PNP) and the Director and the Deputy Director for Administration of the Criminal Investigation and Detection Group (CIDG) powers to issue subpoenas in relation to investigations. A letter request from an "Assistant MCIU-CIDG" is not a subpoena as contemplated by this law.

<sup>6</sup> *Dimal and Castillo v. People*, G.R. No. 216922, April 18, 2018. Even with a search warrant, the police may not conduct a fishing expedition for "objects unspecified".

<sup>7</sup> Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 18(c).

<sup>8</sup> Data Privacy Act of 2012, Section 11.

[Emphases supplied]

However, PNP did not declare the specifics how “a copy of certification” and “any records” will be used for a legitimate purpose.

The request is excessive.

The request for a certification on the individual’s “connection” with UP is excessive because PNP already declared in its letter that the individual was “██████████” of UP. The rules state:<sup>9</sup>

“Section 18. *Principles of Transparency, Legitimate Purpose and Proportionality.* –

*x x x*

(c) *Proportionality.* The processing of information shall be adequate, relevant, suitable, necessary, and **not excessive** in relation to a declared and specified purpose. **Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.”**

[Emphases supplied]

PNP’s purpose is already “fulfilled by other means” because PNP’s letter itself declared the “connection” it is asking for.

The request for “any records” is also excessive because PNP may only collect information “*to the minimum extent necessary to achieve the specific purpose, function, or activity of the public authority.*”<sup>10</sup> Asking for any records is not the “minimum” necessary for PNP’s purpose. Rather, it is a broad and unspecific request which violates the privacy principle of proportionality.

***The concerned individual has the right to be informed of the disclosure of his personal information***

Any future disclosure of the individual’s personal information must be communicated to him. He has “a right to be informed whether personal data pertaining to him or her shall be, are

---

<sup>9</sup> Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 11.

<sup>10</sup> NPC Advisory Opinion No. 2017-50, 29 August 2019.

being, or have been processed”.<sup>11</sup> This is to grant the individual to exercise, if justifiable, any claim to his “right to object” against the processing of his personal information.<sup>12</sup>

### **Suggested course of action**

It is suggested that the reply to the requesting PNP officer be succinct in order to avoid any allegation that UP is reasoning in favor of the individual. UP may simply state that while it supports the PNP in its endeavors, it unfortunately cannot grant the request as is constrained to comply with Article III Section 2 of the 1987 Constitution.

Please feel free to reach out for clarifications or additional concerns.

Yours,

**(Sgd.) Elson B. Manahan**  
Data Protection Officer  
University of the Philippines Diliman

---

<sup>11</sup> Implementing Rules and Regulations of the Data Privacy Act of 2012, Section 34(a)(1).

<sup>12</sup> *Idem*, Section 34 (b).