PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2024 - 007[1]

02 July 2024

[redacted]

Re: DISCLOSURE AND RELEASE OF INCIDENT REPORTS BY AN EDUCATIONAL INSTITUTION.

Dear [redacted]

We respond to your request for guidance on the release of incident reports containing personal information of individuals.

Specifically, you seek guidance on whether Calayan Educational Institution, Inc. (CEFI) may release incident reports under the following circumstances:

1. Sans any court order, is it permissible under the Data Privacy Act and other existing regulations to release incident reports to parties directly involved in the incidents, knowing that personal information of other individuals may be disclosed within these reports?

2. Sans any court order, is it permissible under the Data Privacy and other existing regulations to release incident reports to parties not directly involved in the incidents but mentioned in said reports, knowing that personal information of other individuals may be disclosed within these reports?

3. What should CEFI do to safeguard the right to privacy of individuals whose personal information is contained within incident reports when considering request for copies of or access to such reports?

4. What specific protocols or procedures should requesting parties follow or adhere to when seeking access to or copies of incident reports, particularly in cases where personal information of other individuals may be disclosed.

[1] Incident reports; court order; proportionality; law enforcement.

5. Can CEFI be held liable for refusing to release incident reports despite request from involved parties or those mentioned in the reports?

6. Can the Office of the Prosecutor and other government agencies such as the Department of Education (DepEd) and/ or the Commission on Higher Education (CHED) compel the production or release of reports or other documents containing personal and/or other confidential information in conducting investigations and/or in aid of cases/ complaints filed before them?

7. During investigations conducted by government agencies such as the DepEd and CHED of complaints filed by or against our institution, may our institution submit evidence containing personal and other confidential information in its defense?

Considering that the issues you present are interrelated, we shall address them jointly in the discussions below.

Lawful criteria for processing; Adherence to Data Privacy Principles

The disclosure or sharing of personal and sensitive personal information (collectively, personal data) is considered as processing under the Data Privacy Act of 2012 (DPA). An incident report is a document which contains sensitive personal information because it necessarily involves information concerning an infraction committed or alleged to have been committed by an individual.[2] In NPC Advisory Opinion 2020-013[3] we stated that processing of sensitive personal information shall be considered lawful when it fulfills any one of the criteria listed under Section 13 of the DPA.

In response to questions 1, 2, 6 and 7, in general, the processing of sensitive personal information is prohibited, unless it is necessary for the protection of lawful rights and interests of natural or juridical persons in proceedings, or for the establishment, exercise or defense of legal claims, or when provided to government or public authority in the exercise of their mandate.[4] Therefore, disclosure of sensitive personal information is permissible even without a court order if based upon the foregoing circumstances regardless if the disclosure is made to those directly involved, those merely mentioned, or to public authorities in the exercise of their mandate.

But as we stated in NPC Advisory Opinion 2018-071,[5] even if the DPA recognizes processing of personal data pursuant to the mandate of government agencies, the processing must still adhere to the principles of transparency, legitimate purpose, and proportionality. Personal information must be 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 purpose only. This means that the phrase, "necessary for law enforcement purposes" found in paragraph (e), Section 4 of the DPA is not a weapon that can be indiscriminately wielded by any agency that invokes it. The law enforcement agency must establish its mandate to enforce a particular law, and more importantly, that they are not unreasonably infringing on the rights of individuals guaranteed

[2] Data Privacy Act 2021, § 3 (l) (2).
[3] National Privacy Commission, NPC Advisory Opinion No. 2020-013 (21 February 2020).
[4] Ibid. § 13
[5] National Privacy Commission, NPC Advisory Opinion No. 2018--071 (5 October 2018).

by the Constitution. Failure to establish both grounds renders the processing unnecessary and contrary to law.[6]

We wish to emphasize that an incident report serves to paint a full picture of the truth behind what transpired, and ultimately to advance the lawful rights and interests of those involved. Thus, withholding necessary and vital information under the guise of protecting privacy rights would render its purpose nugatory.

Protocols in Data Protection

In response to questions 3, 4 and 5, the manner of exercising a data subject's right to access would vary from every Personal Information Controller (PIC). As such, there is no catch-all protocol to be followed. An educational institution such as CEFI, however, is required to draft organizational policies that will uphold the rights of the data subject including their right to access. PICs are empowered to establish such reasonable standards and guidelines for data protection and implementation which include the limitation of such rights. Among others, a PIC may limit the exercise of data subject rights when a legitimate purpose exists in justifying such limitation. An example of such limitation may include restriction of certain information through redaction. This limitation on the data subjects' rights is based on the principle of proportionality[7] which essentially provides that the processing of information should be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. You may check our website at privacy.gov.ph for additional resources and guidance on procedures and policies concerning a data subject's right to access. Moreover, a PIC should also keep in mind other governing laws from other regulators in crafting its protocols.

In all cases, however, the restrictions should be in proportion to the purpose of such limitation.[8] For instance, where a PIC denies or limits the exercise of data subject rights, the PIC should ensure that the data subject is clearly and fully informed of the reason for the limitation or denial.[9] CEFI as a PIC can be held liable for an unjustified refusal to release incident reports to concerned parties.

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.

For your reference.

Very truly yours,

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

[6] National Privacy Commission, NPC Advisory Opinion No. 2023-18 (29 September 2023).
[7] Data Privacy Act 2021, § 11
[8] National Privacy Commission, NPC Advisory Opinion No. 2021-001 (19 January 2021).
[9] Ibid.