Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-031[1]

5 August 2021

[redacted]

RE: PROCESSING FOR DUE DILIGENCE, QUALITY CONTROL, AND COMPLIANCE CHECKS PURSUANT TO THE REQUIREMENTS OF THE GOVERNMENT PROCUREMENT REFORM ACT

Dear [redacted]

We write in response to your request received by the National Privacy Commission (NPC) asking for guidance on the propriety of requiring Private Security Agencies (PSA) declared as lowest bidder to submit the latest copy of their Monthly Disposition Reports (MDR) submitted to the PNP Supervising Office for Security and Investigation Agencies (PNP SOSIA) and the PNP Firearms and Explosives Office (FEO) Juridical Firearms License.

We understand that this requirement is pursuant to the conduct of Post Qualification Bid (PQB) and Technical Inspection and Acceptance (TIA) processes of the Civil Aviation Authority of the Philippines (CAAP) Security and Intelligence Service (CSIS) implementing the requirements of Republic Act (RA) No. 9184 also known as the Government Procurement Reform Act[2] (GPRA) and its Implementing Rules and Regulations (IRR).

We understand further that an MDR is a report indicating the names of the PSA's guards assigned to its clients and an updated summary of total number of its employed/deployed guards. On the other hand, a PNP FEO Juridical Firearms License is a document issued to PSAs by the PNP FEO that indicates the list of firearms and its specifications (calibre type, make, model and serial number), registration, and authorized ownership.

Finally, we understand that the CSIS is requiring the aforementioned documents to determine the following:

[1] Tags: criteria for lawful processing; legal obligation; mandate; copyright; general data privacy principles.
[2] An Act Providing For The Modernization, Standardization, And Regulation Of The Procurement Activities Of The Government And For Other Purposes. [Government Procurement Reform Act], Republic Act No. 9184 (2002).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL: https://www.privacy.gov.ph/ Email Add: info@privacy.gov.ph * Tel No. 8234-2228

1. Whether security guards deployed in CAAP airports and facilities are duly licensed and included in the MDRs submitted to the PNP SOSIA; and
2. Whether the personal protection equipment (firearm) they carry are authentic and duly registered and licensed by PNP FEO.

Scope of the Data Privacy Act; criteria for lawful processing of personal data; legal obligation

The Data Privacy Act of 2012[3] (DPA) applies to the processing of personal information,[4] sensitive personal information,[5] and privileged information[6] (collectively, personal data) of natural persons by the government and private entities and individuals, within and outside the Philippines.

We would like to highlight that while an MDR involves personal data protected under the DPA, a PNP FEO Juridical Firearms License is issued to juridical entities. We wish to clarify that the DPA only applies to the processing of personal data of natural persons and not information of juridical entities recognized under the law, such as corporations, associations, and partnerships.[7] Thus, the DPA does not apply to the processing of information which pertains to a license issued to a juridical person.

Nevertheless, the processing of personal data in the MDR should have a lawful basis under the DPA. Section 12 and 13 of the DPA provides for criteria in processing personal data. Particularly in your case, the following provision may apply, viz:

> "SECTION 12. Criteria for Lawful Processing of Personal Information. — The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists: x x x
>
> (c) The processing is necessary for compliance with a **legal obligation** to which the personal information controller is subject; x x x
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to **fulfill functions of public authority** which necessarily includes the processing of personal data for the fulfillment of its mandate; or x x x
>
> SECTION 13. Sensitive Personal Information and Privileged Information. — The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases: x x x

[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], (2012).

[4] *Id.* § 3 (g): 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.

[5] *Id.* § 3 (l): Sensitive personal information refers to personal information:
(1) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
(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) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
(4) Specifically established by an executive order or an act of Congress to be kept classified.

[6] *Id.* § 3 (k) Privileged information refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

[7] National Privacy Commission, NPC Advisory Opinion No. 2021-027 (July 2021).

(b) The processing of the same is **provided for by existing laws and regulations**: Provided, That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: Provided, further, That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information; x x x."

On whether the CSIS may require PSAs to submit their latest MDRs without violating the DPA, the IRR of the GPRA is highly instructive. Section 34.3, Rule X of the same provides, to wit:

"RULE X – POST-QUALIFICATION

Section 34. Objective and Process of Post-Qualification

x x x

34.3 The post-qualification shall verify, validate, and ascertain all statements made and documents submitted by the bidder with the Lowest Calculated Bid/Highest Rated Bid, using non-discretionary criteria, as stated in the Bidding Documents. These criteria shall consider, but shall not be limited to, the following:

a) Legal Requirements. **To verify, validate, and ascertain licenses, certificates, permits, and agreements submitted by the bidder**, and the fact that it is not included in any "blacklist" as provided in Section 25.3 of this IRR. For this purpose, the GPPB shall maintain a consolidated file of all "blacklisted" suppliers, contractors, and consultants. x x x"

Considering that verification of legal requirements is part of the Post Qualification process in government procurement, the same is recognized as a legitimate purpose for processing personal data. It goes without saying that the processing of the MDR is in compliance with a legal obligation under current procurement laws and/or necessary for the fulfillment of the mandate of the CAAP. Thus, CAAP may validly require a PSA to submit the latest copy of its MDR as a post qualification requirement without violating the DPA.

Lastly, CAAP, as a personal information controller, is required to adhere to the general data privacy principles, implement reasonable and appropriate safeguards to protect personal data collected from the PSAs against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing, and uphold data subject rights.

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