Republic of the Philippines
NATIONAL PRIVACY COMMISSION

NPC Circular No. 2022 – 03

DATE : **05 December 2022**

SUBJECT : **GUIDELINES FOR PRIVATE SECURITY AGENCIES ON THE PROPER HANDLING OF CUSTOMER AND VISITOR INFORMATION**

WHEREAS, the National Privacy Commission (NPC) recognizes the vital role of Private Security Agencies (PSA) and Security Guards in ensuring the safety and security of persons and properties;

WHEREAS, entities classified as personal information controllers (PICs) under Republic Act No. 10173 or the Data Privacy Act of 2012 (DPA), generally engage PSAs and Security Guards to secure and control access to identified areas or properties, among others;

WHEREAS, the NPC received reports concerning the apparent disregard by some Security Guards of the data privacy rights of customers, visitors, and other data subjects;

WHEREAS, pursuant to the Philippine National Police-Supervisory Office for Security and Investigation Agencies Memorandum dated 15 June 2020 and the Housing and Land Use Regulatory Board Administrative Order 3, Series of 2017 dated 19 May 2017, PSAs and other similar entities engaged by homeowners' associations (HOA) do not have the authority to require motorists to surrender their driver's license, even temporarily, as a condition for entry to gated communities, as such authority is lodged by law[1] only upon the Land Transportation Office (LTO) or others it may deputize;

WHEREAS, the sole purpose for requiring an Identification Card (ID) from the customers, visitors, and other data subjects is to verify their identity;

WHEREAS, there is a need to inform and acquaint PSAs and Security Guards with the proper processing of personal data during the performance of their duties to avoid violating the rights of data subjects under the DPA;

WHEREAS, Section 11 of the DPA allows the processing of personal information subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the general principles of transparency, legitimate purpose, and

[1] Land Transportation and Traffic Code, § 29: Confiscation of Driver's License. – Law enforcement and peace officers of other agencies duly deputized by the Director shall, in apprehending a driver for any violation of this Act or any regulations issued pursuant thereto, or of local traffic rules and regulations not contrary to any provisions of this Act, confiscate the license of the driver concerned and issue a receipt prescribed and issued by the Bureau therefor which shall authorize the driver to operate a motor vehicle for a period not exceeding seventy-two hours from the time and date of issue of said receipt. The period so fixed in the receipt shall not be extended, and shall become invalid thereafter. Failure of the driver to settle his case within fifteen days from the date of apprehension will be a ground for the suspension and/or revocation of his license.

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

proportionality;

WHEREAS, Section 14 of the DPA states that a PIC may subcontract the processing of personal information: *provided*, that the PIC shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of the DPA and other laws for processing of personal information;

WHEREAS, Section 21 (a) of the DPA further states that a PIC is accountable for complying with the requirements of the law and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party;

WHEREAS, PSAs and Security Guards engaged by a PIC are considered personal information processors (PIPs) and are also bound to observe the requirements of the DPA and other applicable laws;

WHEREAS, pursuant to Section 7 of the DPA, the NPC is charged with the administration and implementation of the provisions of the law, which includes ensuring the compliance by PICs with the provisions of the DPA, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

WHEREAS, Section 9 of the Implementing Rules and Regulations of the DPA (IRR) provides that the Commission shall, among its other functions, develop, promulgate, review or amend rules and regulations for the effective implementation of the law;

WHEREFORE, in consideration of the foregoing premises, and without prejudice to the application of other pertinent laws and regulations on the matter, the NPC hereby issues this Circular that prescribes the guidelines for PICs as well as PSAs and Security Guards acting as PIPs, on the proper handling of data subjects' personal data.

SECTION 1. ***Scope***. **—** This Circular shall apply to all PICs, and to PSAs and Security Guards acting as PIPs, in the processing of personal data of customers, visitors, and other data subjects as part of their security services.

SECTION 2. ***Definition of Terms***. **—** The definition of terms in the DPA and its IRR, as amended, are adopted herein. In addition, whenever used in this Circular, the following terms shall mean or be understood as follows:

A. "Private Security Agency" or "PSA" refers to any person or entity engaged in contracting, recruitment, training, furnishing, or posting of Security Guards and other private security personnel to individuals, corporation, offices, and organizations, whether private or public, for their security needs as the Philippine National Police (PNP) may approve;[2]

B. "Security Guard" refers to any person who offers or renders personal service to watch or secure either a residence, business establishment, buildings, compounds, areas, or property, inspects, monitors, or performs bodily checks or searches of individuals or

[2] See: Department of Labor and Employment, Revised Guidelines Governing the Employment and Working Conditions of Security Guards and other Private Security Personnel in the Private Security Industry, Department Order No. 150-16, series of 2016 [DOLE DO No. 150-16], § 2 (i) (Feb. 9. 2016).

baggage, and other forms of security inspection,[3] as authorized by the PIC or by the PSA to perform such functions, regardless of his or her designation;

C. "Service Agreement" refers to the contract between the PIC and the PSA acting as a PIP containing the terms and conditions governing the performance or completion of security service, jobs, or work being farmed out for a definite or predetermined period;[4]

D. "Subcontracting" refers to the outsourcing, assignment, or delegation of the processing of personal data by a PIC to a PIP. In this arrangement, the PIC retains control over the processing;

E. "Subcontracting Agreement" refers to a contract, agreement, or any similar document which sets out the obligations, responsibilities, and liabilities of the parties to a subcontracting arrangement. It shall contain mandatory stipulations prescribed by the IRR.

SECTION 3. ***General Obligations of PICs engaging the services of PSAs.*** **—** All PICs engaging the services of PSAs shall have the following obligations:

A. *Transparency.* PICs, in coordination with the PSAs, shall be responsible for developing a privacy notice in clear and plain language which shall explain to all customers, visitors, and other data subjects:

1. The purpose of collecting personal data, e.g., monitoring or controlling access to premises for the security, safety, and protection of persons and properties, pursuant to legitimate interests (for private sector PICs) or laws and regulations (for government PICs);
2. The security measures implemented to safeguard personal data;
3. The fact that the personal data collected, whether manually or through electronic systems, shall be turned over to the pertinent PIC who engaged the PSA or the Security Guard;
4. The retention period of personal data; and
5. Their rights as a data subject and mechanisms on how to exercise the same;

B. *Proportionality.* PICs shall observe proportionality in all personal data processing activities including those outsourced or subcontracted to PSAs. They shall not require PSAs acting as PIPs as well as the Security Guards to access, record, copy, or otherwise collect any sensitive personal information for purposes of ascertaining the identity of an individual, nor shall they direct them to keep ID cards containing sensitive personal information.

However, PICs may instruct PSAs and authorized Security Guards to visually examine a government-issued ID within a reasonable time: *provided,* that there is prior sufficient explanation to the data subject of the necessity of processing sensitive personal information for that purpose: *provided further*, that the government-issued ID shall not be kept by the PSA or authorized Security Guards.

C. *Accountability.* PICs shall use contractual or other reasonable means to ensure that proper safeguards are in place to guarantee the confidentiality, integrity, availability of the

[3] *Id.* § 2 (h).
[4] DOLE DO No. 150-16, § 2 (j).

personal data processed, and to prevent its use for unauthorized purposes. PICs shall ensure that a Subcontracting Agreement or Service Agreement is executed with PSAs prior to any personal data processing activity. Such agreement shall contain the following:

1. The subject-matter and duration of the processing;
2. The nature and purpose of the processing;
3. The type/s of personal data that will be processed;
4. The categories of data subjects;
5. The geographic location of the processing under the agreement;
6. The obligations and rights of PICs;
7. The specific obligations of PSAs taking into consideration the mandatory stipulations under Section 44 (b) of the IRR of DPA; and
8. The duty of PSAs to comply with the requirements of the DPA and its IRR, other relevant issuances of the Commission, other applicable laws, and any other obligations with the PICs.

D. *Safeguards.* PICs shall ensure that reasonable and appropriate safeguards are in place for the processing of personal data by PSAs and their Security Guards which include, but are not limited to:

1. Appropriate data protection policies that provide for organizational, physical, and technical security measures, taking into account the nature, scope, context and purpose of the processing, as well as the risks posed to the rights and freedoms of data subjects;
2. Clear and adequate instructions on the processing of personal data, whether in paper-based or electronic systems, including the strict protocols to be observed by Security Guards in the processing of sensitive personal information, where justified, as provided under Section 3(B) of this Circular;
3. Reasonable retention period of personal data as well as the method to be adopted for the secure return, destruction, or disposal of the same and the timeline therefor, taking into account the purpose for which the personal data was obtained and the provisions of the applicable Subcontracting Agreement or Service Agreement.
    a. The retention of personal data shall only be limited to the time necessary for the fulfillment of the declared, specified, and legitimate purpose/s, or when the processing relevant to the purpose has been terminated.
    b. For government agencies, the retention period under the applicable law shall be observed.[5]

SECTION 4. ***Obligations of PSAs acting as PICs.*** **—** All PSAs acting as PICs shall have the following obligations:

A. *Registration.* All PSAs acting as PICs shall register with the Commission in accordance with the applicable Rules on the Registration of Data Processing Systems and Notifications regarding Automated Decision-Making;

B. *Training.* PSAs shall provide trainings on the DPA, its IRR, and other relevant issuances of the Commission to all Security Guards prior to their assignment or deployment.

[5] See: National Archives of the Philippines, General Records Disposition Schedule common to all Government Agencies, series 2009 which provides for the retention period of two (2) years after date of last entry for logbooks (available at https://nationalarchives.gov.ph/wp-content/uploads/2015/04/NAP-Gen.-Circular-1-2-and-GRDS-2009.pdf).

1. The orientation shall include an overview on the proper handling of personal data that comes to their knowledge and possession in the course of providing security services, the requirement to maintain confidentiality, integrity, and availability of personal data, and the corresponding sanctions for any unauthorized processing of personal data;
2. The conduct of the training shall be properly documented at all times. The Commission may require the submission of the same in accordance with the applicable provisions of the DPA, its IRR, and other issuances on the matter;

C. *Inspection*. All PSAs shall ensure that all Security Guards assigned or deployed are complying with the requirements of the DPA. For this purpose, PSAs shall conduct regular onsite visits in establishments where its Security Guards are assigned or deployed.

SECTION 5. *Obligations of PSAs acting as PIPs.* — All PSAs acting as PIPs shall have the following obligations:

A. *Privacy Notice*. PSAs shall make reasonable efforts to notify the data subjects of the relevant information about the processing of their personal data through a privacy notice developed by the PIC in coordination with the PSAs.

B. *Proportionality.* For purposes of ascertaining the identity of an individual, PSAs and authorized Security Guards shall not access, record, copy, or otherwise collect any sensitive personal information such as date of birth, government-issued ID numbers, images of government-issued IDs, nor shall they keep ID cards containing sensitive personal information.

However, PSAs and authorized Security Guards may be allowed to examine a government-issued ID within a reasonable time: *provided,* that there is prior sufficient explanation to the data subject of the necessity of processing sensitive personal information for that purpose: *provided further*, that the government-issued ID shall not be kept by the PSA or authorized Security Guards.

C. *Security measures*. PSAs and their Security Guards shall, in coordination with the PIC, implement appropriate security measures that:

1. Aim to maintain the availability, integrity, and confidentiality of personal data processed;
2. Provide adequate protection against any accidental or unlawful destruction, alteration, disclosure, and unlawful processing, as well as against natural and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

PSAs and Security Guards shall, at all times, ensure that entries consisting of personal data in the logbooks, health forms, and other records are not visible to or accessible by unauthorized persons, employees, or other data subjects to prevent unlawful processing of personal data.

D. *Assistance.* PSAs acting as PIPs and its Security Guards shall cooperate with the relevant PIC in addressing any requests for the exercise of data subject rights. PSAs shall not engage another PIP without prior instruction from the PIC.

E. *Inspection*. PSAs acting as PIPs shall allow audits and inspections conducted by the PIC or another auditor authorized by such PIC.

SECTION 6. ***Penalties***. — The processing of personal data in violation of this Circular shall carry criminal, civil, and administrative liability pursuant to the provisions of the DPA and related issuances of the Commission. This is without prejudice to the administrative penalties that may be imposed under Republic Act No. 5487 or "An Act to Regulate the Organization and Operation of Private Detective, Watchmen or Security Guards Agencies" and other applicable laws.

SECTION 7. ***Interpretation.*** —Any doubt in the interpretation of any provision of this Circular shall be liberally interpreted in a manner mindful of the rights and interests of the data subjects.

SECTION 8. ***Transitory Provisions.*** — PICs and PSAs acting as PIPs shall be given a period of sixty (60) days from the effectivity of these Guidelines to comply with the requirements provided herein.

SECTION 9. ***Separability Clause.*** — If any portion or provision of this Circular is declared null and void, or unconstitutional, the other provisions not affected thereby shall continue to be in force and effect.

SECTION 10. ***Repealing Clause.*** — All other rules, regulations, and issuances contrary to or inconsistent with the provisions of this Circular are deemed repealed or modified accordingly.

SECTION 11. ***Effectivity.*** — This Circular shall take effect fifteen (15) days after its publication in the Official Gazette or a newspaper of general circulation.

Approved:

SGD.
JOHN HENRY D. NAGA
Privacy Commissioner

SGD.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner