Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2018-003

15 January 2018

[redacted]

RE: VISITOR LOGBOOK

Dear [redacted],

This pertains to your query received by the National Privacy Commission (NPC) via NPC's official *Facebook* page. Particularly, you inquired about the following:

1. Appropriate means to regulate the visitor logbooks for security purposes;
2. Whether consent is needed in collecting personal information; and
3. Registration of the logbook with the NPC.

In your inquiry, you have mentioned that for every visitor entering the building or office, you require them to provide certain information in the logbook, such as: (1) name; (2) time of arrival; (3) time of departure; and (4) signature, and visitors are likewise required to surrender one (1) government-issued identification card, in exchange for the visitor's pass.

These information are considered as personal and sensitive personal information under the Data Privacy Act of 2012 (DPA).[1] Specifically, the name and signature of the individual or visitor are considered as personal information. [2] On the other hand, the government-issued identification card containing the number specifically assigned to the individual by the issuing government agency is considered as sensitive personal information.[3]

Given that you are processing personal and sensitive personal information as mentioned above, the DPA then directs you, as the personal information controller, to comply with duties and responsibilities under the law and implement appropriate security measures to ensure the protection and security of such personal data.[4]

[1] Republic Act No. 10173, An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and in the Private Sector, Creating for this purpose a National Privacy Commission and for other purposes, "Data Privacy Act of 2012" (15 August 2012).
[2] *Id.*, §3(g).
[3] *Id.*, §3(l).
[4] *Id.*, §21.

It is imperative to determine whether the information being collected in the logbooks are necessary and proportionate to the purpose of collection. Following such determination, the risks and vulnerabilities in the processing should likewise be identified and addressed, and an evaluation of the current security measures being implemented should be made to see if these are reasonable and appropriate to ensure the security and protection of personal information or whether there is a need to improve current practices. These may be accomplished through the conduct of privacy impact assessment.

To observe the principle of transparency to the data subjects, a privacy notice or privacy statement may be displayed alongside the logbook to apprise the visitors of the purpose of collection, recipients of collected information and retention period of stored information, among others.

Kindly note that Singapore's data protection authority, the Personal Data Protection Commission (PDPC), has decided a complaint in relation to the failure by a security company to safeguard their visitor logbook which resulted to a data breach incident.[5] The PDPC ruled that the recording and safekeeping of logbooks were considered as activities involving processing of personal data, hence, actual processes, practices and policies must be put in place in order to protect personal data and ensure the safety of the logbook at all times.[6]

With regards to consent of data subjects, a personal information controller may lawfully process personal information if the circumstance falls under any of the criteria for lawful processing of personal information, consent being one of them.[7] Legitimate interest is also a criterion for processing personal information. Please refer to Section 13 of the DPA for the criteria for lawful processing of sensitive personal information.

On the registration requirement, NPC issued a circular – *Registration of Data Processing Systems and Notifications Regarding Automated Decision-Making,*[8] Section 5 of which provides:

> "SECTION 5: Mandatory Registration. A PIC or PIP shall register its data processing system if it is processing personal data and operating in the country under any of the following conditions:
>
> A. The PIC or PIP employs at least two hundred fifty (250) employees;
>
> B. The processing includes sensitive personal information of at least one thousand (1,000) individuals;
>
> C. The processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:

[5] Investigation under Section 50(1) of the PDPA 2012 and MCST 3696. Eagle Eye, Case Number: DP-1610-B0275, 29 June 2017. Available at https://www.pdpc.gov.sg/docs/default-source/enforcement-data-protection-cases/grounds-of-decision---eagle-eye---290617.pdf?sfvrsn=2. (Last accessed 13 December 2017)

[6] *Id.*

[7] *Supra note* 1, §12.

[8] See NPC Circular No. 2017-01

1. Information that would likely affect national security, public safety, public order, or public health;
2. Information required by applicable laws or rules to be confidential;
3. Vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exits in the relationship between a data subject and PIC or PIP;
4. Automated decision-making; or
5. Profiling

D. The processing is not occasional: *Provided,* that processing shall be considered occasional it is only incidental to the mandate or function of the PIC or PIP, or, it only occurs under specific circumstances and is not regularly performed. Processing that constitutes a core activity of a PIC or PIP, or is integral thereto, will not be considered occasional."

Thus, if you satisfy any of the above-mentioned conditions, you are required to register with the NPC. For Sections 5(C) and (D) above, please note also the Appendix to the circular providing for the initial list of specific sectors, industries, or entities that shall be covered by mandatory registration.

It is important to note that the definition of a data processing system[9] includes manual or paper-based systems, i.e. logbooks, as well as electronic systems.

Finally, we wish to emphasize that data collection through visitor logbooks may often be overlooked. But as this a paper-based processing system, security measures to protect the data need not be a complicated matter as this will entail reasonable and appropriate organizational and physical security measures only.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner and Chairman

[9] Implementing Rules and Regulations (IRR) of the RA No. 10173, §3(e).