Republic of the Philippines
NATIONAL PRIVACY COMMISSION

REMINDER TO PERSONAL INFORMATION CONTROLLERS REGARDING TAKING OF PICTURES OF IDENTIFICATION DOCUMENTS

The National Privacy Commission draws attention to prevalent practices by certain businesses and associations (both Personal Information Controllers and Personal Information Processors) of authorizing, allowing, or acquiescing its employees, agents, or personnel in taking the identification (ID) cards of customers, guests, or other persons using their personal electronic devices, or without appropriate safeguards, and/or without the required privacy notice.

To illustrate, here are some examples of these practices:

- Hotel receptionists taking photos of guest IDs using their personal smartphones instead of company-issued phones;
- Car sales agents taking photocopies of the ID of a potential customer for verification purposes;
- Agents of a telcos requesting a potential customer to send a photo of the customer's ID via private communication such as Viber, WhatsApp, or Facebook Messenger; and
- Homeowners and condominium associations taking copies and requiring the deposit of physical IDs with Sensitive Personal Information without appropriate policies and security measures for their PIP security agency to implement.

The Commission emphasizes that these types of activities carry a great risk of causing security incidents, data breaches, unauthorized uses, inadequate disposal, lack of informed consent, and profiling or discrimination, among others.

PICs/PIPs shall obtain the consent of the data subjects prior to the collection and processing of their personal data, subject to exemptions provided by the DPA and other applicable laws and regulations.[1] It is the duty of the PICs, as well as their employees, agents, or representatives, to uphold the confidentiality and privacy of the personal data that they process.

To this end, the Commission mandates the following practices:

- **Consent:** Where it is the necessary criteria for lawful processing of Sensitive Personal Information under Sections 13 of the DPA, the PIC must obtain explicit consent from individuals to capture and process their identification photos and details.

- **Privacy Notice:** Provide a clear, understandable, and transparent privacy notice before capturing their IDs. The notice should include the purposes of the processing, the security measures implemented, the retention period, and the purpose limitation, among others.

- **Secure Storage and Transmission**: Implement policies to ensure that photos taken by personal devices are stored in a manner that is in compliance with company policies and the

[1] Section 19 of the Implementing Rules and Regulations of the Data Privacy Act of 2012.

DPA. Implement safeguards that ensure that the photos cannot be used by the employees, agents, or personnel for other purposes, such as encryption, access controls, and other tools.

- **Proper Disposal**: Establish policies and procedures that ensure the disposal and deletion of the photos once the purpose is fulfilled. The PIC should conduct verification and audits to ensure that disposal policies have been complied with.

We reiterate that processing personal data violative of the Data Privacy Act of 2012 and related issuances of the Commission is subject to penalties and administrative fines.

###