ZICO | law

ASEAN INSIDERS
by origin and passion

LEGAL ALERT

**Philippines**
**3 December 2018**


**Author**

**Felix Sy**
Managing Partner
Insights Philippines
Legal Advisors (IPLA)
felix.sy@insights-law.com

**Lorybeth Baldrias-Serrano**
Partner
Insights Philippines
Legal Advisors (IPLA)
lorybeth.serrano
@insights-law.com


# Guidelines on Data Privacy Compliance Checks

Data privacy is a relatively new regulation in the Philippines. Nonetheless, the Philippine National Privacy Commission ("NPC") is exerting its best efforts in order to enforce data privacy laws in the Philippines. In its stage of infancy, the NPC has taken on a stance of educating and enabling controllers and processors to comply with data privacy laws. Its efforts have gained the NPC local and international recognition, respect and credibility notwithstanding being a new and young agency.

Further to the NPC's mandate of monitoring compliance of natural or juridical person or other body involved in processing personal data, specifically their security measures, on 20 September 2018, it issued NPC Circular No. 18-02, which lays out guidelines regarding the conduct of data privacy compliance checks. .

The Compliance checks will be performed for the following purposes:

1. Protect individuals and their personal data by cultivating a culture of privacy in all agencies, companies and organizations involved in the processing of personal data;
2. Effectively implement data privacy laws by strengthening the regulatory environment in the country and the NPC's ability to identify and take action on non-compliance, with the interest and welfare of the people as a primary consideration; and
3. Emphasize accountability, to the end that personal information controllers ("PIC") and personal information processors ("PIP") are allowed to demonstrate compliance with data privacy laws, and to promote the building of trust between data subjects and processors of personal data, whether the government or the private sector.

For the key highlights of the circular, please see below:

## Modes of Compliance Checks

The NPC may employ any of the following modes of compliance checks:

1. *Privacy Sweep.* The NPC shall review a PIC or PIP's compliance with data privacy laws based on publicly available information, such as websites, mobile applications, raffle coupons, brochures, and privacy notices. This is the initial mode of compliance check.
2. *Documents Submission*. The NPC may require submission of documents and additional information from a PIC or PIP that has undergone a privacy sweep to clarify findings arising therefrom, and to determine the level of compliance of the PIC or PIP.
3. *On-Site Visit*. The NPC may subject a PIC or PIP to an on-site visit if there are persistent or substantial findings of non-compliance with data privacy laws.

The circular also provides considerations that the NPC will consider in conducting a compliance check against a PIC or PIP:

1. Level of risk to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;
2. Reports received by the NPC against the PIC or PIP;
3. Non-registration of a PIC or PIP that is subject to the mandatory registration requirement as provided under NPC Circular No. 17-01;

4. Unsecured or publicly available personal data found on the internet that may be traced to a PIC or PIP; and
5. Other considerations that indicate non-compliance with data privacy laws.

It is important to note that based on any of the foregoing considerations, the NPC may, in its discretion, directly employ an on-site visit if the totality of circumstances warrant such action.

The NPC shall send a Notice of Compliance Check, accompanied with a Privacy Compliance Questionnaire, to a PIC or PIP regarding the conduct of a compliance check through the e-mail address used at the time they registered with the NPC. Such notice shall be deemed received on the next business day. A Notice of Compliance Check will be sent in the following instances:

1. Documents Submission. The Notice will require the submission of specific documents or policies in a machine-readable or other commonly used file format, within a given period of time, which shall not be less than 10 days. This period stated in the Notice will be determined based on the nature of the findings in the Privacy Sweep.
2. On-Site Visit. The Notice shall be sent to the PIC or PIP at least 10 days before such visit. It shall include an order for the presentation of documents or records, conduct of interviews, inspection of premises and equipment, and other necessary activities.

### Notice of Deficiency, Compliance Order, Certificate of No Significant Findings

If the PIC or PIP is found to be non-compliant with data privacy laws, the NPC shall issue a Notice of Deficiencies indicating the period of time within which to correct the identified deficiencies, which shall not be less than 10 days. If after the lapse of this period, the PIC or PIP did not take any action or that such identified deficiencies persist, the NPC will issue a Compliance Order. Compliance Orders shall state the deficiencies remaining or actions to be taken, the period within which to undertake the corrections ordered by the NPC, and the period to report such actions.

On the other hand, the NPC shall issue a Certificate of No Significant Findings to a PIC or PIP that has undergone Document Submission or an On-site Visit, where no substantial deficiencies were found or the deficiencies identified in the Notice of Deficiencies have been addressed to the satisfaction of the NPC. This Certificate is without prejudice to any other recommendation being made by the NPC for the improvement of the PIC or PIP's compliance with data privacy laws. The issuance of this Certificate also does not bar an investigation for any possible liability arising from complaints and/or personal data breaches filed before the NPC.

### Refusal to Undergo Compliance Check or Failure to Comply with Compliance Order

A PIC or PIP who, without good reason and despite due notice, refuses or prevents the NPC from performing a compliance check may be subject to appropriate sanctions as may be allowed by law, such as fines and penalties as may be appropriate. Furthermore, deficiencies that are not corrected by the PIC or PIP within the prescribed period stated in the Compliance Order may subject the PIC or PIP to criminal, civil or administrative penalties, without prejudice to other remedies available under the law.

If you have any questions or require any additional information, please contact Felix Sy or Lorybeth Baldrias Serrano or the ZICO Law partner you usually deal with.

*This alert is for general information only and is not a substitute for legal advice.*