NPC Circular No. 18-02 – Guidelines on Compliance Checks

PDF VERSION	:	npc-circular-18-02-guidelines-on-compliance-checks
DATE	:	20 September 2018
SUBJECT	:	Guidelines on Compliance Checks

WHEREAS, The right to privacy, which includes information privacy, is constitutionally protected and accorded recognition independent of its identification with liberty, and at the same time, Article II, Section 11 of the Constitution values the dignity of every human person and guarantees full respect for human rights;

WHEREAS, Article II, Section 24, of the Constitution provides that the State recognizes the vital role of communication and information in nation-building, and Section 2 of Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), provides that it is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth;

WHEREAS, Section 7 of the DPA provides that the National Privacy Commission (Commission) shall administer and implement the provisions of the DPA, monitor and ensure compliance of the country with international standards set for data protection, and ensure compliance of Personal Information Controllers with the provisions of the DPA, and Section 14 of the DPA also requires Personal Information Processors to comply with all the requirements of the Act and other applicable laws;

WHEREAS, Section 7 of the DPA provides that the Commission can compel any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy, or coordinate with government and the private sector in implementing plans and policies to strengthen personal data protection;

WHEREAS, in order to ensure compliance of the country and all PICs and PIPs with the law and international standards set for data protection, including adherence to data privacy principles, implementation of security measures, and provisions for data subjects to exercise their rights, Section 29 of the Implementing Rules and Regulations (IRR) provides that the Commission shall monitor the compliance of natural or juridical person or other body involved in the processing of personal data, specifically their security measures.

WHEREFORE, in consideration of these premises, the Commission hereby issues this Circular governing the conduct of Compliance Checks.

Back to Top

I. GENERAL PROVISIONS

SECTION 1. *Scope*. These Rules shall apply to any Personal Information Controller (PIC) or Personal Information Processor (PIP) in the government or private sector processing personal data in the Philippines, subject to the relevant provisions of the DPA, its IRR, and the relevant issuances and orders of the NPC.

SECTION 2. *Purpose*. These Rules provide the guidelines for the conduct of Compliance Checks by personnel of the Commission, whichever mode it may be. Compliance Checks are undertaken for the following purposes:

A. 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;
B. Effectively administer and implement the DPA by strengthening the regulatory environment in the country and the Commission's ability to identify and take action on non-compliance, with the interest and welfare of the people as a primary consideration; and,
C. To emphasize the importance of accountability, to the end that PICs and PIPs are allowed the opportunity to demonstrate compliance with the DPA, its IRR and relevant rules and regulations, and to promote the building of trust between data subjects and those involved in the processing of personal data, whether the government or the private sector.

Back to Top

SECTION 3. *Definition of Terms*. For the purpose of this Circular, the following terms are defined, as follows:

A. "Act" or "DPA" refers to Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012;

B. "Certificate of No Significant Findings" refers to an issuance of the Commission to a Personal Information Controller or Personal Information Processor which serves as a certification that it has undergone a Compliance Check and there were no notable findings requiring further action from the Commission.

The Certificate also refers to an issuance which certifies that an entity has undergone a Compliance Check with findings of substantial deficiencies, and has implemented remediation measures as ordered by the Commission.

C. "Commission" or "NPC" refers to the National Privacy Commission;

D. "Compliance Check" refers to the systematic and impartial evaluation of a PIC or PIP, in whole or any part, process or aspect thereof, to determine whether activities that involve the processing of personal data are carried out in accordance with the standards mandated by the Data Privacy Act and other issuances of the Commission. It is an examination, which includes Privacy Sweeps, Documents Submissions and On-Site Visits, intended to determine whether a PIC or PIP is able to demonstrate organizational commitment, program controls and review mechanisms intended to assure privacy and personal data protection in data processing systems.

E. "Compliance Order" refers to an issuance of the Commission to a PIC or PIP directing it to perform actions, institute measures or any other prescriptions of the Commission in relation to the Compliance Check conducted.

F. "Data Processing System" refers to a structure and procedure by which personal data is collected and further processed in an information and communications system or relevant filing system, including the purpose and intended output of the processing;

G. "Data Protection Officer" refers to an individual designated by the head of agency or organization to be accountable for its compliance with the Act, its IRR, and other issuances of the Commission;

H. "Document Submission" refers to a mode of Compliance Check as defined under Section 4 (B) of this Circular.

I. "IRR" refers to the Implementing Rules and Regulations of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012.

J. "Notice of Deficiencies" refers to a document issued by the Commission indicating the deficiencies of a PIC or PIP found to be non-compliant upon the conduct of a Compliance Check, taking into consideration the provisions of the DPA, its IRR, and the relevant issuances and orders of the NPC;

K. "On-Site Visit" refers to a mode of Compliance Check as defined under Section 4 (C) of this Circular.

L. "Personal Data" refers to all types of personal information, and sensitive personal information as defined under R.A. No. 10173.

M. "Personal Information Controller" (PIC) refers to a natural or juridical person, or any other body that controls the processing of personal data, or instructs another to process personal data on its behalf.

N. "Personal Information Processor" (PIP)(PIP) refers to any natural or juridical person or any other body to whom a personal information controller may outsource or instruct the processing of personal data pertaining to a data subject.

O. "Privacy Compliance Questionnaire" is a document containing a series of questions formulated by the Commission to be answered by the PIC or PIP to contextualize documents and policies that the Commission requires to be submitted.

P. "Privacy Sweep" refers to a mode of Compliance Check as defined under Section 4 (A) of this Circular.

Back to Top

II. GUIDELINES FOR THE CONDUCT OF COMPLIANCE CHECK

SECTION 4. *Modes of Compliance Checks*. In ensuring compliance with the Act and its related issuances, the Commission may employ any of the following modes of Compliance Checks:

A. *Privacy Sweep*. The Commission shall review a PICs or PIPs compliance with respect to its obligation under the DPA, and its related issuances based on publicly available or accessible information, such as, but not limited to, websites, mobile applications, raffle coupons, brochures, and privacy notices. This is the initial mode of Compliance Check.

B. *Documents Submission*. The Commission may require the submission of documents and additional information from a PIC or PIP that has undergone a privacy sweep to, among others, clarify certain findings arising therefrom, and to determine the level of compliance of the PIC or PIP with respect to its obligations under the DPA and its related issuances.

C. *On-site Visit*. The Commission may subject a PIC or PIP to an on-site visit if there are persistent or substantial findings of non-compliance with the obligations indicated in the DPA and its related issuances.

Authorized personnel of the Commission shall conduct a targeted inspection within the premises of a PIC or PIP that may include a presentation of documents or records, visits to selected departments wherein processing of personal information are undertaken, as well as interviews of relevant personnel tasked to handle personal information processed by the PIC or PIP subject to the Compliance Check.

The Commission may, in its discretion, directly employ this mode of Compliance Check if it determines that the totality of circumstances warrant such action, taking into account the next succeeding provision.

Back to Top

SECTION 5. *Considerations for the Conduct of Compliance Checks*. A PIC or PIP in the government or private sector may be subject to a Compliance Check based on any of the following considerations:

a) Level of risk to the rights and freedoms of data subjects posed by personal data processing by a PIC or PIP;

b) Reports received by the Commission against the PIC or PIP; or its sector;

c) Non-registration of a PIC or PIP that is subject to the mandatory registration requirement as provided under NPC Circular 17-01;

d) Unsecured or publicly available personal data found on the internet that may be traced to a PIC or PIP; and

e) Other considerations that indicate non-compliance with the DPA or the issuances of the Commission.

In cases where the Complaints and Investigations Division (CID) of the Commission is investigating or commences an investigation against a PIC or PIP undergoing or scheduled for Compliance Check, the Compliance Check shall be held in abeyance and the investigation shall be given precedence.

Back to Top

SECTION 6. *When to Conduct Compliance Check*. An On-Site Visit may be conducted during regular office hours except Saturdays, Sundays and legal holidays. Privacy Sweep, Documents Submission, or investigations conducted by the CID are not subject to such limitations; Provided, if the last day of the period to comply with an order for Document Submission, falls on a Saturday, a Sunday, or a legal holiday, the last day shall be the next working day.

SECTION 7. *Notice of Compliance Checks*. The Commission shall send a Notice, accompanied with a Privacy Compliance Questionnaire, to a PIC or PIP regarding the conduct of a Compliance Check through the electronic mail (e-mail) address used at the time they registered with the Commission. Such Notice shall be deemed received on the next business day; Provided, for unregistered organizations, the Notice shall be sent to their registered business address via courier addressed to the head of the organization.

A PIC or PIP shall take the necessary steps to ensure that their registered e-mail address is working and able to receive the Notice promptly.

A Notice of Compliance Check will be sent in the following instances:

a) *Documents Submission*. The Commission shall send a Notice to the PIC or PIP requiring 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 ten (10) days. This period stated in the Notice will be determined based on the nature of the findings in the Privacy Sweep.

b) *On-site Visit*. The Commission shall send a Notice to the PIC or PIP at least ten (10) days before such visit. The Notice shall include an Order for the Presentation of Documents or Records, Conduct of Interviews, Inspection of Premises and Equipment and other necessary activities.

The on-site visit team shall bring an Order from the Commission identifying those authorized to conduct the inspection, and shall display proper identification tags issued by the Commission.

SECTION 8. *Issuance of Notice of Deficiencies*. If the PIC or PIP is found to be non-compliant with the DPA, its IRR, and other issuances of the Commission, the Commission shall issue a Notice of Deficiencies indicating the period of time within which to correct the identified deficiencies, which shall not be less than ten (10) days. The DPO, or in the case of unregistered entities, the head of the organization, shall file with the Commission a report on the actions taken.

Back to Top

SECTION 9. *Issuance of Compliance Order*. The Commission shall issue a Compliance Order in the following instances:

a) After the lapse of the period provided in the Notice of Deficiencies and no action was taken by the PIC or PIP to correct the identified deficiencies.

b) After the lapse of the period provided in the Notice of Deficiencies and such identified deficiencies persist.

If the persistence of the deficiencies is due to the considerable period of time or resources needed to implement the necessary remediation measures, the timeline to complete such measures, as approved by the Commission, shall be embodied in a Compliance Order.

c) In the course of the conduct of an on-site visit, the PIC or PIP refuses or fails to provide access to premises, records or prevents the conduct of the inspection.

Compliance Orders shall state the deficiencies remaining or actions to be taken, the period within which to undertake the corrections ordered by the Commission, and the period to report such actions.

Back to Top

SECTION 10. *Issuance of Other Orders*. The Commission may issue any and all pertinent orders in connection with the conduct or furtherance of a Compliance Check or the assessment of any organization's compliance with any orders in relation thereto.

SECTION 11. *Certificate of No Significant Findings*. The Commission 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 already been addressed to the satisfaction of the Commission.

The issuance of this Certificate is without prejudice to any other recommendation being made by the Commission for the improvement of the organization's compliance with the DPA and related issuances. The issuance of this Certificate does not bar an investigation for any possible liability arising from complaints and/or personal data breaches filed before the Commission.

SECTION 12. *Failure to Comply with Compliance Order*. 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.

SECTION 13. *Refusal to Undergo Compliance Check*. A PIC or PIP who, without good reason and despite due notice, refuses or prevents the Commission from performing a Compliance Check may be subject to appropriate sanctions as may be allowed by law. In case of refusal, the following provisions shall govern:

A. *Action to be Taken upon Refusal or Failure to Comply with Documents Submission and Complete the Privacy Compliance Questionnaire*. Refusal or failure to submit the requested documents or policies, or submit a completed Privacy Compliance Questionnaire, within the period stated in the Notice or Order, shall subject a PIC or PIP to an on-site visit from the Commission, enforcement actions, and such other fines and penalties as may be appropriate under the circumstances.

B. *Action to be Taken upon Refusal or Failure to Provide Access to Premises or Records during an On-site Visit*. Refusal or failure to provide access to premises or records during an on-site visit shall subject a PIC or PIP to a Compliance Order, enforcement actions, and such other fines and penalties as may be appropriate under the circumstances.

C. *Failure or Refusal to Provide an Explanation to Compliance Orders*. Refusal or failure to submit an explanation to the Order cited in the preceding paragraphs, or if the explanation does not present a compelling reason to justify such refusal or failure, may subject a PIC or PIP to contempt proceedings, as may be permitted by law, before the appropriate court, or such other actions as may be available to the Commission.

SECTION 14. *Fines and Penalties*. Failure to comply with the DPA, other issuances, or orders of the Commission may subject a PIC or PIP to fines and penalties as may hereafter be prescribed by the Commission.

Back to Top

III. MISCELLANEOUS PROVISIONS

SECTION 15. *Publication*. To protect the public, and in keeping with the Commission's mandate to inform the public on data subject rights, as well as the compliance of PICs and PIPs with their obligations under the law, the results of the Compliance Checks, and orders issued in relation thereto may be published by the Commission at its discretion.

SECTION 16. *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 17. *Effectivity Clause*. This Circular shall take effect immediately after publication in the Official Gazette or two (2) newspapers of general circulation.

Approved:

(Sgd.) RAYMUND E. LIBORO
Privacy Commissioner

(Sgd.) IVY D. PATIDU
Deputy Privacy Commissioner

(Sgd.) LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Date: **20 September 2018**

Back to Top