

CLIENT ALERT:

For Immediate Compliance: Appointment of a Data Protection Officer

The National Privacy Commission (NPC) issued NPC Advisory No. 2017-01 on the *Designation of Data Protection Officers*¹ pursuant to Section 21(b) of the Data Privacy Act of 2012 (R.A. No. 10173)² and Rule VI, Section 26(a) of its Implementing Rules and Regulations³. The advisory sets forth the guidelines on the mandatory appointment by all personal information controllers (PICs) and personal information processors(s) of a data protection officer (DPO). While the relevant guidelines have only been recently issued, compliance therewith should be immediate, based on the NPC ruling that the period for complying with the Data Privacy Act of 2012 expired in 2013 or one (1) year after the effective date of the law⁴.

Qualifications of a DPO

Each PIC or PIP is required to appoint a DPO who will be accountable for ensuring their organization's compliance with the Data Privacy Act of 2012, its Implementing Rules and Regulations, NPC issuances, and other laws on privacy and data protection.

An individual PIC or PIP is automatically the DPO.

A PIC or PIP, which is juridical entity, is required to appoint one (1) DPO for its entire organization. It may also appoint a Compliance Officer for Privacy (COP) for each of its branches, sub-offices, or other component units.

Subject to the approval of the NPC, a group of related companies may appoint a common DPO for ensuring compliance by the entire group, provided that each member company shall have a COP who will be under the direct supervision of the DPO.

The position of a DPO or COP shall have the following qualifications:

- (1) Expertise in relevant privacy or data protection policies and practices;
- (2) Sufficient understanding of their organization's processing operations, information systems, data security, and/or data protection needs;
- (3) A full-time or organic employee of the PIC or PIP;
- (4) A regular or permanent employee of the PIC or PIP; who should hold at least a 2-year employment contract with their organization; and
- (5) Independent in the exercise of his or her functions such that the performance of their duties will not give rise to a conflict of interests⁵.

Functions and Duties of a DPO or COP

A DPO has the following minimum responsibilities:

- (a) monitor the PIC's or PIP's compliance with the Data Privacy Act, its Implementing Rules and Regulations, NPC issuances, and other applicable laws and policies;

(b) ensure the conduct of Privacy Impact Assessments⁶ relative to activities, measures, projects, programs, or systems of the PIC or PIP;

(c) advise the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights;

(d) ensure proper data breach and security incident management by the PIC or PIP, including the latter's preparation and timely submission to the NPC of reports and other documentation concerning security incidents or data breaches;

(e) inform and cultivate awareness on privacy and data protection within the organization of the PIC or PIP, including all relevant laws, rules and regulations and NPC issuances;

(f) advocate for the development, review and/or revision of policies, guidelines, projects and/or programs of the PIC or PIP relating to privacy and data protection, by adopting a privacy by design⁷ approach;

(g) serve as the contact person of the PIC or PIP vis-à-vis data subjects, the NPC, and other authorities in all matters concerning data privacy or security issues or concerns;

(h) cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and

(i) perform other duties and tasks that may be assigned by the PIC or PIP that will further the interest of data privacy and security and uphold the rights of the data subjects.

Except for items (a) to (c), a COP shall also have the foregoing duties and functions.

The PIC or PIP may outsource or subcontract the duties of the DPO or COP, provided that the DPO or COP shall oversee the performance by the service provider. The DPO shall also remain the contact person of the PIC or PIP on data privacy matters.

Obligations of the PIC or PIP

Upon the appointment of its DPO and COPs, the PIC or PIP has the following obligations:

(i) effectively communicate to its personnel, the designation of the DPO or COP and their functions;

(ii) allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;

(iii) provide sufficient time and resources necessary for the DPO or COP to keep themselves updated with the developments in data privacy and security and to carry out their tasks effectively and efficiently;

(iv) grant the DPO or COP appropriate access to the personal data the PIC or PIP is processing, including its processing systems;

(v) where applicable, invite the DPO or COP to participate in meetings of senior and middle management to represent the interest of privacy and data protection;

(vi) promptly consult the DPO or COP in the event of a personal data breach or security incident;

(vii) ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities; and

(viii) publish the contact details of the DPO or COP in, *at least*, the following materials:

- a. website;
- b. privacy notice;
- c. privacy policy; and
- d. privacy manual or privacy guide.

Actions to Consider

Considering the current effectivity of the Data Privacy Act of 2012 and its Implementing Rules and Regulations, PICs and PIPs are urged to immediately appoint a DPO who meets the qualifications prescribed by the NPC.

A group of companies may consider appointing either: (1) a DPO per member company or (2) subject to NPC's approval, a common DPO who will directly supervise the COP of each member company.

PICs and PIPs who are required to register their data processing systems with the NPC on or before 9 September 2017 shall be required to commence the registration process by submitting to the NPC information regarding their respective DPOs and COPs, together with copies of their appointment papers.

The NPC is presently preparing for the imminent launch of the online registration portal which is now on beta testing at <http://register.privacy.gov.ph/Registry>. The launch of the online registration tool is expected to be preceded by, or simultaneous with, the issuance by the NPC of the official registration guidelines. Our Firm is closely monitoring the progress of these activities of the commission. Clients are encouraged to stay alert for updates on further developments.

¹Available at: <https://privacy.gov.ph/advisories/npc-advisory-no-2017-01-designation-data-protection-officers/>.

²SEC. 21. *Principle of Accountability*. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) xxx xxx xxx

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

³Section 26. *Organizational Security Measures*. Where appropriate, personal information controllers and personal information processors shall comply with the following guidelines for organizational security:

a. Compliance Officers. Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer, compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security.

xxx xxx xxx

⁴*In Re: Investigation of the Data Breach Involving COMELEC Website and/or Data Processing System* (NPC Case No. 16-001, 28 December 2016).

⁵"Conflict of Interest" refers to a scenario in which a DPO is charged with performing tasks, duties, and responsibilities that may be opposed to or could affect his performance as DPO. This includes, inter alia, holding a position within the PIC or PIP that leads him to determine the purposes and the means of the processing of personal data. The term shall be liberally construed relative to the provisions of the Advisory.

⁶"Privacy Impact Assessment" is a process undertaken and used to evaluate and manage the impact on privacy of a particular project, program, process or measure.

⁷"Privacy by Design" is an approach to the development and implementation of projects, programs, and processes that integrates into the latter's design or structure safeguards that are necessary to protect and promote privacy, such as appropriate organizational, technical, and policy measures.

Contact Us



Bienvenido A. Marquez III

Partner
Intellectual Property
Practice Group

Bienvenido.Marquez@quisumbingtorres.com



Divina V. Ilas-Panganiban

Partner
Intellectual Property
Practice Group

Divina.Ilas-Panganiban@quisumbingtorres.com



Neonette E. Pascual

Associate
Intellectual Property
Practice Group

Neonette.Pascual@quisumbingtorres.com