Republic of the Philippines
NATIONAL PRIVACY COMMISSION

# NPC Advisory No. 2017-01

**DATE : 14 MARCH 2017**

**SUBJECT : DESIGNATION OF DATA PROTECTION OFFICERS**

## Preamble

**WHEREAS**, Article II, Section 24 of the 1987 Constitution provides that the State recognizes the vital role of communication and information in nation-building. At the same time, Article II, Section 11 thereof stresses that the State values the dignity of every human person and guarantees full respect for human rights. Finally, Article XIII, Section 21 states that Congress shall give highest priority to the enactment of measures that protect and enhance the right of the people to human dignity;

**WHEREAS**, 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. The State also recognizes its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected;

**WHEREAS**, Section 21(b) of the DPA and Section 50(b) of its Implementing Rules and Regulations (IRR) provide that personal information controllers (PICs) shall designate an individual or individuals who are accountable for the organization's compliance with this Act. Section 14 of the DPA and Section 45 of the IRR also require personal information processors (PIPs) to comply with all the requirements of the Act and other applicable laws, including issuances by the NPC;

**WHEREAS**, pursuant to Section 26(a) of the IRR, 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 (DPO), compliance officer, or shall otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security;

**WHEREAS**, pursuant to Section 7 of the DPA, the National Privacy Commission (NPC) is charged with the administration and implementation of the provisions of the law, which includes ensuring compliance with the provisions of the DPA and with international standards for data protection, and carrying out efforts to formulate and implement plans and policies that strengthen the protection of personal information in the country, in coordination with other government agencies and the private sector;

**WHEREAS**, Section 4 of NPC Circular 2016-01 declares that a government agency engaged in the processing of personal data shall, through its head of agency, designate a DPO;

**WHEREAS**, in consideration of the foregoing premises, the NPC hereby issues this Advisory that prescribes the guidelines for the designation of a DPO:

## Scope

These Guidelines shall apply to all natural or juridical persons, or any other body in the government or private sector engaged in the processing of personal data within and outside of the Philippines, subject to the applicable provisions of the DPA, its IRR, and issuances by the NPC.

## Definition of Terms

Whenever used in this Advisory, the following terms shall have their respective meanings as hereinafter set forth:

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

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

c. "Compliance Officer for Privacy" or "COP" refers to an individual or individuals who shall perform some of the functions of a DPO, as provided in this Advisory;

d. "Conflict of Interest" refers to a scenario wherein 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 this Advisory;

e. "Data Sharing Agreement" refers to a contract, joint issuance, or any similar document that contains the terms and conditions of a data sharing arrangement between two or more parties: *Provided*, that only personal information controllers shall be made parties to a data sharing agreement;

f. "Data Subject" refers to an individual whose personal, sensitive personal, or privileged information is processed;

g. "Government Agency" refers to a government branch, body, or entity, including national government agencies, bureaus, or offices, constitutional commissions, local government units, government-owned and controlled corporations, government financial institutions, state colleges and universities;

h. "Personal data" refers to all types of personal information, including privileged information;

i. "Personal information" refers to any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual;

j. "Personal information controller" or "PIC" refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

   1.) a person or organization who performs such functions as instructed by another person or organization; or
   2.) an individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

   There is control if the natural or juridical person or any other body decides on what information is collected, or the purpose or extent of its processing;

k. "Personal information processor" or "PIP" refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject;

l. "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;

m. "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;

n. "Privileged Information" refers to any and all forms of data which, under the Rules of Court and other pertinent laws, constitute privileged communication;

o. "Processing" refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data;

p. "Sensitive Personal Information" refers to personal information:

   1.) About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

   2.) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

3.) Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and

4.) Specifically established by an executive order or an act of Congress to be kept classified.

## General Principles

These Guidelines shall be governed by the following general principles:

a. The responsibility for complying with the Act, its IRR, issuances by the NPC, and all other applicable laws lies with the PIC or PIP.[1] When necessary, it must be capable of demonstrating its capacity to comply.

b. The DPO or COP shall act independently in the performance of his or her functions, and shall enjoy sufficient degree of autonomy. For this purpose, he or she must not receive instructions[2] from the PIC or PIP regarding the exercise of his or her tasks.

c. The DPO or COP is bound by secrecy or confidentiality concerning the performance of his or her tasks.

## Mandatory Designation

A PIC or PIP shall designate an individual or individuals who shall function as DPO. The DPO shall be accountable for ensuring the compliance by the PIC or PIP with the DPA, its IRR, issuances by the NPC, and other applicable laws and regulations relating to privacy and data protection.

In certain cases, a PIC or PIP is allowed to designate a compliance officer for privacy (COP):

a. *Local Government Units (LGUs)*. Each LGU shall designate a DPO. However, a component city, municipality, or *barangay* is allowed to designate a COP, provided that the latter shall be under the supervision of the DPO of the corresponding province, city, or municipality that that component city, municipality or *barangay* forms part of.

b. *Government Agencies*. Each government agency shall designate a DPO. Where a government agency has regional, provincial, district, city, municipal offices, or any other similar sub-units, it may designate or appoint a COP for each sub-unit. The COPs shall be under the supervision of the DPO.

[1] RA 10173, §21(a), and §14.
[2] e.g., what results should be achieved, how to investigate a complaint, whether to consult the NPC, what view or interpretation of the law to take relative to a specific data protection issue, etc.

c. *Private Sector*. Where a private entity has branches, sub-offices, or any other component units, it may also appoint or designate a COP for each component unit.

   Subject to the approval of the NPC, a group of related companies may appoint or designate the DPO of one of its members to be primarily accountable for ensuring the compliance of the entire group with all data protection policies. Where such common DPO is allowed by the NPC, the other members of the group must still have a COP, as defined in this Advisory.

d. *Other Analogous Cases*. PICs or PIPs that are under similar or analogous circumstances may also seek the approval of the NPC for the appointment or designation of a COP, in lieu of a DPO.

An individual PIC or PIP shall be a *de facto* DPO.

## General Qualifications

The DPO should possess specialized knowledge and demonstrate reliability necessary for the performance of his or her duties and responsibilities. As such, the DPO should have expertise in relevant privacy or data protection policies and practices. He or she should have sufficient understanding of the processing operations being carried out by the PIC or PIP, including the latter's information systems, data security and/or data protection needs.

Knowledge by the DPO of the sector or field of the PIC or PIP, and the latter's internal structure, policies, and processes is also useful.

The minimum qualifications for a COP shall be proportionate to his or her functions, as provided in this Advisory.

## Position of the DPO or COP

The DPO or COP should be a full-time or organic employee of the PIC or PIP.

In the government or public sector, the DPO or COP may be a career or appointive position.

In the private sector, the DPO or COP should ideally be a regular or permanent position.[3] Where the employment of the DPO or COP is based on a contract, the term or duration thereof should at least be two (2) years to ensure stability.

In the event the position of DPO or COP is left vacant,[4] the PIC or PIP should provide for the appointment, reappointment, or hiring of his or her replacement within a reasonable period of time. The PIC or PIP may also require the incumbent DPO or COP to occupy such position in an holdover capacity until the appointment or hiring of a new DPO or COP, in

[3] Consultants and project, seasonal, probationary, or casual employees should not be designated as DPOs.
[4] In the event of resignation, incapacity, or death of the DPO, or, where the term of the DPO is fixed or is coterminous with the appointing authority, in the case of government agencies, or based on a contract, in the case of private sector entities.

accordance with the PIC or PIP's internal policies or the provisions of the appropriate contract.

## Independence, Autonomy And Conflict of Interest

A DPO or COP must be independent in the performance of his or her functions, and should be accorded a significant degree of autonomy by the PIC or PIP.

In his or her capacity as DPO or COP, an individual may perform (or be assigned to perform) other tasks or assume other functions[5] that do not give rise to any conflict of interest.

## Duties and Responsibilities Of the DPO and COP

A DPO shall, *inter alia*:

a. monitor the PIC's or PIP's compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies. For this purpose, he or she may:

    1.) collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
    2.) analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
    3.) inform, advise, and issue recommendations to the PIC or PIP;
    4.) ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
    5.) advice the PIC or PIP as regards the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the law;

b. ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;

c. advice the PIC or PIP regarding complaints and/or the exercise by data subjects of their rights (e.g., requests for information, clarifications, rectification or deletion of personal data);

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

[5] The designated DPO may also occupy some other position in the organization (e.g., legal counsel, risk management officer, etc.).

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 issuances of the NPC;

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 design 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 and the PIC or PIP;

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 perform all other functions of a DPO. Where appropriate, he or she shall also assist the supervising DPO in the performance of the latter's functions.

The DPO or COP must have due regard for the risks associated with the processing operations of the PIC or PIP, taking into account the nature, scope, context and purposes of processing. Accordingly, he or she must prioritize his or her activities and focus his or her efforts on issues that present higher data protection risks.

## General Obligations of the PIC or PIP Relative to the DPO or COP

The PIC or PIP should:

a. effectively communicate to its personnel, the designation of the DPO or COP and his or her functions;

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

c. provide sufficient time and resources (financial, infrastructure, equipment, training, and staff) necessary for the DPO or COP to keep himself or herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;

d. grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;

e. 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;

f. promptly consult the DPO or COP in the event of a personal data breach or security incident; and

g. ensure that the DPO or COP is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.

## Outsourcing or Subcontracting of Functions

A PIC or PIP may outsource or subcontract the functions of its DPO or COP. However, to the extent possible, the DPO or COP must oversee the performance of his or her functions by the third-party service provider or providers. The DPO or COP shall also remain the contact person of the PIC or PIP vis-à-vis the NPC.

## Protections

To strengthen the autonomy of the DPO or COP and ensure the independent nature of his or her role in the organization, a PIC or PIP should not directly or indirectly penalize or dismiss the DPO or COP for performing his or her tasks. It is not necessary that the penalty is actually imposed or meted out. A mere threat is sufficient if it has the effect of impeding or preventing the DPO or COP from performing his or her tasks. However, nothing shall preclude the legitimate application of labor, administrative, civil or criminal laws against the DPO or COP, based on just or authorized grounds.

## Publication and Communication Of Contact Details

To ensure that its own personnel, the data subjects, the NPC, or any other concerned party, is able to easily, directly, and confidentially contact the DPO or COP, a PIC or PIP must publish the DPO's or COP's contact details in, *at least*, the following materials:

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

A PIC or PIP may introduce or offer additional means of communicating (e.g., telefax, social media platforms, etc.) with its DPO or COP.

For this purpose, the contact details of the DPO or COP should include the following information:

a. title or designation
b. postal address
c. a dedicated telephone number
d. a dedicated email address

The name or names of the DPO or COP need not be published. However, it should be made available upon request by a data subject or the NPC.

## Weight of Opinion

The opinion of the DPO or COP must be given due weight. In case of disagreement, and should the PIC or PIP choose not to follow the advice of the DPO or COP, it is recommended, as good practice, to document the reasons therefor.

## Accountability

While the responsibility of complying with the DPA, its IRR, issuances by the NPC, and other applicable laws remains with the PIC or PIP, malfeasance, misfeasance, or nonfeasance on the part of the DPO or COP relative to his designated functions may still be a ground for administrative, civil, or criminal liability, in accordance with all applicable laws.

Approved:

**(Sgd.) RAYMUND E. LIBORO**
Privacy Commissioner

**(Sgd.) IVY D. PATDU**
Deputy Privacy Commissioner

**(Sgd.) DAMIAN DOMINGO O. MAPA**
Deputy Privacy Commissioner

Date: 14 March 2017