



Republic of the Philippines
DEPARTMENT OF ENERGY
(Kagawaran ng Enerhiya)

DEPARTMENT ORDER NO. DO2017-08-0011

CREATION OF THE DATA PRIVACY COMMITTEE

In compliance with Republic Act No. 10173, also known as the Data Privacy Act of 2012 and its Implementing Rules and Regulations, a Data Privacy Committee is hereby established to facilitate the formulation and implementation of the Data Privacy Program of the Department. The following are the designated members of the Data Privacy Committee:

Data Protection Officer (DPO)	-	Director, ITMS
Compliance Officer for Privacy (COP)	-	Director, Legal Services
Personal Information Controller (PIC)	-	All Bureau Directors All Services Directors Field Offices Directors
Personal Information Processors (PIP)	-	All Division Chiefs

Pursuant to the National Privacy Commission (NPC) Advisory No. 2017-01 dated March 14, 2017 prescribing the guidelines for the designation of a Data Privacy Officer, the following are the duties and responsibilities of the designated DPO, CPO, PIC and PIP:

A. Data Protection Officer

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

2. Ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
3. Advise 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);
4. 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. 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;
6. 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;
7. 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;
8. Cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
9. 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.

B. Compliance Officer for Privacy

Except for items (1) to (3), the COPs shall perform all other functions of the DPO. Where appropriate, COPs also assist the supervising DPO in the performance of his 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, they must prioritize their activities and focus their efforts on issues that present higher data protection risks.

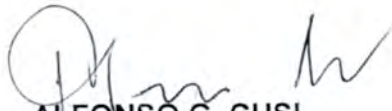
C. General Obligations of the PIC or PIP Relative to the DPO or COP

The PIC or PIP should:

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

2. allow the DPO or COP to be involved from the earliest stage possible in all issues relating to privacy and data protection;
3. 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;
4. grant the DPO or COP appropriate access to the personal data it is processing, including the processing systems;
5. 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;
6. promptly consult the DPO or COP in the event of a personal data breach or security incident; and
7. 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.

This Department Order shall take effect immediately and shall remain in effect until revoked by the undersigned and/or by competent authority.


ALFONSO G. CUSI
Secretary



Republic of the Philippines
DEPARTMENT OF ENERGY
IN REPLYING PLS. CITE:

DOE-AGC-17004039



AUG 29 2017