



Republic of the Philippines  
**OFFICE OF THE SECRETARY**  
 Elliptical Road, Diliman 1100 Quezon City  
 +63(2) 8928-8741 to 64 and +63(2) 8273-2474

**SPECIAL ORDER**

No. 419  
 Series of 2024

**SUBJECT : CREATION OF THE DATA PRIVACY COMMITTEE IN THE DEPARTMENT OF AGRICULTURE**

In compliance with Republic Act (R.A.) No. 10173, otherwise known as the “Data Privacy Act of 2012”, its Implementing Rules and Regulations, as well as the existing issuances of the National Privacy Commission (NPC) appurtenant thereto, a **Data Privacy Committee** (DPC or this Committee) headed by the Data Privacy Officer (DPO) is hereby created in furtherance of the Data Privacy compliance initiatives of the Department of Agriculture (DA).

Pursuant to NPC Advisory No. 2017-01 dated 14 March 2017, entitled “Designation of Data Protection Officers”, the Data Privacy Committee shall be **independent** in the performance of their functions, and should be accorded a significant degree of **autonomy** by the Personal Information Controller (PIC) or the Personal Information Processor (PIP). For purposes of this Special Order, it is understood that the Department of Agriculture (DA) is the PIC.

**I. COMPOSITION**

<b>Data Privacy Officer (DPO)</b>	: Director, Legal Service <sup>1</sup>
<b>Compliance Officers for Privacy</b>	: Representative, Office of the Secretary Director, Field Operations Service (FOS) Program Director, Special Area for Agricultural Development (SAAD) Program Head, i-Support Group, Philippine Rural Development Project (PRDP) Regional Technical Directors for Operations (RTDs), Regional Field Offices (RFOs) Two (2) Attorney III, Research and Regulations Division (RRD), Legal Service One (1) Attorney III, Litigation and Adjudication (LAD), Legal Service

<sup>1</sup> The Data Protection Officer of this Department is Atty. Willie Ann M. Angsiy, Director IV of the Legal Service, pursuant to Special Order No. 832, series of 2023.

<p><b>Data Protection and Breach Response Team</b></p> <p>Head (DA- Central Office)</p> <p>Head (RFOs)</p> <p>Members</p>	<p>: Director, Information and Communications Technology Service (ICTS)</p> <p>: Regional Executive Directors (REDs)</p> <p>: Chief, Network Operations and Management Division (NOMD), ICTS</p> <p>Head, Information Communication technology Unit (ICTU)</p>
<p><b>Secretariat</b></p>	<p>: Two (2) technical staff from the ICTS</p> <p>One (1) technical staff from the Legal Service</p> <p>One (1) technical staff from the Administrative Service</p>

## II. DUTIES AND RESPONSIBILITIES

### A. Compliance Officers for Privacy (COPs)

In accordance with NPC Circular No. 2022-04, entitled *Registration of Personal Data Processing System, Notification Regarding Automated Decision-Making or Profiling, Designation of Data Protection Officer, and the National Privacy Commission Seal of Registration*, COPs shall be under the direct supervision of the DPO and shall have the following duties and responsibilities:

1. Assist the DPO in the performance of her functions;
2. Monitor their RFO's or data processing system's<sup>2</sup> compliance with the DPA, its IRR, issuances by the NPC and other applicable laws and policies and submit monthly reports<sup>3</sup> to the DPO;
3. Review documents in connection with data privacy, such as Data Sharing Agreements, in accordance with the DPA, its IRR, and NPC issuances;
4. Upon the instructions of the DPO, collect information to identify the processing operations, activities, measures, projects, programs, or systems of their respective RFOs or data processing systems, and maintain a record thereof;
5. Analyze and check the compliance of processing activities;
6. Conduct a preliminary assessment of the propriety of issuing security clearances to and compliance by third-party service providers, and provide recommendations to the DPO;

<sup>2</sup> For RFOs, the COP is their respective RTD for Operations. For data processing systems of such as but not limited to the RSBSA, SAAD, Human Resource and Personnel, the COP will be their respective Directors.

<sup>3</sup> Submissions shall be made not later than the 5<sup>th</sup> day after the end of each month.

7. Assist the DPO in issuing data protection advice and recommendations to the PIC or PIP;
8. Ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing;
9. Confer with and assist the DPO in ascertaining the necessity of executing a Data Sharing Agreement with third parties, and ensure its compliance with the DPA, its IRR, and NPC issuances;
10. 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;
11. 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;
12. 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;
13. Serve as the representative of the DPO and the secondary contact person of the PIC or PIP with respect to the RFO or the data processing system 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;
14. Assist the DPO in cooperating, coordinating, and seeking the advice of the NPC regarding matters concerning data privacy and security;
15. Perform other duties and tasks that may be delegated by the DPO in furtherance of data privacy compliance and security and to uphold the rights of the data subjects; and
16. Submit quarterly reports<sup>4</sup> to the DPO detailing his/her performance of the above-enumerated duties and responsibilities.

## **B. Data Protection and Breach Response Team (DPBRT)**

In compliance with NPC Circular No. 16-03 dated 27 December 2016 entitled *Personal Data Breach Management*, the Head of the DPBT shall have the authority to make immediate decisions regarding critical action, if necessary.

Apart from rendering assistance in ensuring that information and data assets are managed securely, the DPBT shall help mitigate the impact of any data breach in the DA. It shall thus perform the following functions:

### **1. Preparation and Planning**

- Develop within 30 days from the date of this issuance a security incident management policy and response plan that details and outlines the steps to be taken if a data breach occurs.
- Conduct risk assessments through identification of potential vulnerabilities and risks to the Department's data and systems.

---

<sup>4</sup> Submissions shall be made not later than the 5<sup>th</sup> day after the end of each quarter.

- Assist in establishing communication protocols that defines how the DBPT will communicate with this Committee and the PIC internally and externally during a breach.

## **2. *Monitoring, Detection, and Assessment***

- Continuously monitor systems and networks for vulnerabilities and potential security threats.
- Recognize when a data breach is in progress or has occurred.
- Determine the scope and nature of the breach and its potential impact.

## **3. *Containment and Mitigation***

- Take immediate action to isolate compromised systems or networks to prevent further damage.

## **4. *Recovery and Remediation***

- Bring affected systems back online and ensure that they are secure.
- Recover and restore lost or compromised data.
- Strengthen security measures to prevent future breaches.

## **5. *Documentation and Reporting***

- Keep detailed records of all actions taken during the incident response process and submit report to the DPO.

## **6. *Training and Awareness***

- Assist in providing training to the employees to raise awareness about data security and how to respond to potential breaches.

### **C. *Heads of Programs/Projects and the Regional Executive Directors (RED)***

Should any of the identified personnel designated as COP or member of the DPBRT be separated from his/her position, designation, or sub-unit, the concerned Head/RED shall immediately nominate a replacement to this Committee for the latter's consideration and approval.

1. Effectively communicate to the personnel within their jurisdiction, the designation of the COP and member of the DPBRT and his or her functions;
2. Allow members of this Committee 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 member of this Committee to keep himself/herself updated with the developments in data privacy and security and to carry out his or her tasks effectively and efficiently;

4. Where applicable, invite the COP/ member of the DPBRT to participate in the meetings of senior and middle management to represent the interest of privacy and data protection;
5. Promptly consult the members of the Committee in the event of a personal data breach or security incident; and
6. Ensure that the COP/ member of the DPBRT is made a part of all relevant working groups that deal with personal data processing activities conducted inside the organization, or with other organizations.


**D. Secretariat**

1. Provide administrative and technical assistance during meetings such as a.) preparing and circulating Notices of Meeting; b.) securing the attendance of the participants; c.) preparing the Minutes of each meeting; d.) keeping formal records and other correspondences; and e.) assisting the DPO and CPOs in preparation of presentation materials during the meetings.
2. Maintain a database and a record of all document, report or any output of this Committee.
3. Perform other duties necessary for the efficient operation of this Committee.

All expenses to be incurred in the conduct of meetings, official travel, per diem, incidental expenses and other related activities shall be chargeable against OSEC funds, subject to the existing government accounting and auditing laws, rules, and regulations.

This Order shall take effect immediately and shall remain in force unless revoked in writing. All other orders, memoranda, and issuances inconsistent herewith are deemed revoked.

Done this 21<sup>st</sup> day of MARCH 2024.

  
**FRANCISCO P. TIU LAUREL, JR.**  
Secretary



DA-CO-OSEC-SO2024G 121-00226