



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

## MEMORANDUM ORDER

No. 87  
Series of 2024

**SUBJECT : DATA PRIVACY MANUAL FOR THE REGISTRY SYSTEM FOR BASIC SECTORS IN AGRICULTURE (RSBSA)**

### I. BACKGROUND

#### THE RSBSA

The Registry System for Basic Sectors in Agriculture (RSBSA) is an electronic compilation (database) of information on DA's primary stakeholders (farmers, farmworkers, fisherfolk, and agri-youth), to wit: personal and socio-economic information, agri-fishery activities and livelihood information, and interventions received and programs/services participated.

Section 41 of the R.A. No. 8435 otherwise known as "Agriculture and Fisheries Modernization Act of 1997" mandates the creation of the National Information Network (NIN). In relation to this, the Registry System for Basic Sector in Agriculture (RSBSA) was adopted based on the Memorandum of Agreement in 2011 between Department of Budget and Management (DBM), Department of Interior and Local Government (DILG), Department of Agrarian Reform (DAR), National Statistics Office (NSO) and Department of Agriculture (DA) and used by DBM to target beneficiaries of different agri-fishery support programs of the government as implemented by various government agencies.

The RSBSA serves as a requirement and basis for implementing various programs such as providing production input and financial assistance, insurance services, and other interventions that cater to Filipino farmers and fisherfolk. Hence, all farmers and fisherfolk registered in the RSBSA are given priority in the targeting and implementation of the respective agency programs in accordance with the special provisions embodied in the General Appropriations Act (GAA).

However, since its conception in 2013, the data listed in the RSBSA has not been updated. Therefore, the pressing need to establish a means to update the registry to address issues of comprehensibility, precision, and accuracy of data allowed the DBM to authorize the DA to spearhead this activity in 2018 through a letter addressed to the DA Secretary, signed by the then DBM Secretary.

For this purpose, the DA developed the national RSBSA Profiling Platform (RSBSAPP), a web-based system designed to allow an efficient, real-time, and accessible updating of the RSBSA. During the last quarter of 2019, the DA prompted the updating of the RSBSA by sending out enrollment forms, instructional manuals, information materials, and operationalizing the RSBSAPP in each DA-RFO. In addition, the official updating of the RSBSA registration protocol to guide the implementation led by the DA-RFOs was authorized pursuant to the Protocol for Registration and Updating of the RSBSA issued on 17 September 2019 (General Documents: OSEC-09-19-9567).

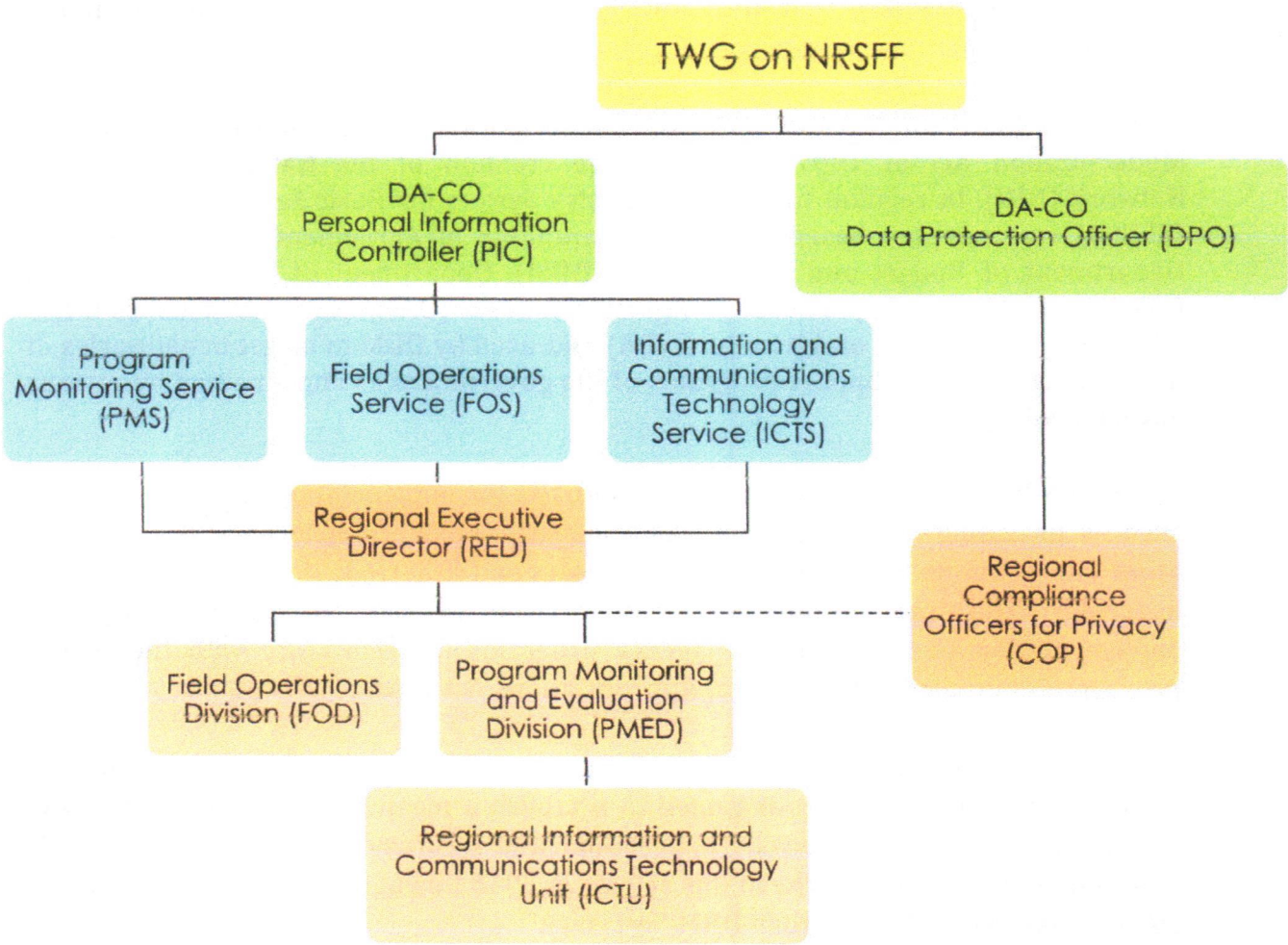


**RSBSA-NPMO AND TWG ON NRSFF**

Through DA Special Order No. 1161, Series of 2018, the creation of a National Program Management Office (NPMO) was established for the purpose of the RSBSA Updating program implementation. The RSBSA-NPMO serves as the office in the DA-Central Office responsible for overseeing and monitoring the program implementation of the RSBSA-Regional Program Management Offices (RPMOs) and cascades unified and systematic protocols and mechanisms to ensure that the program achieves its vision, mission, and objectives.

Above the RSBSA-NPMO is the Technical Working Group on National Registry System for Farmers and Fishers (TWG on NRSFF), created through DA Special Order No. 853, Series of 2020, which facilitates the completion of the updating of the RSBSA. The TWG on NRSFF approves or disapproves activities based on the relevance and appropriateness of the activity to the overall progress of the program.

**ORGANIZATIONAL STRUCTURE OF THE TWG ON NRSFF**



**FUNCTIONS OF THE TWG ON NRSFF**

The TWG on NRSFF has the following functions:

**DA CO – Field Operations Service (FOS)**

- Formulates or update as necessary, the implementation guidelines and protocol for the data collection, registration procedures, and updating of information of



legitimate farmers, farm workers, fisherfolk, and agri-youth in the RSBSA, subject to the approval of the RSBSA-National Program Steering Committee (RSBSA-NPSC);

- Identifies emerging RSBSA concerns related to the profiling of farmers and fisherfolk and devises solutions that may consist of strategic planning, process evaluation, protocol amendment, systems enhancement, organizational change, and/or policy development;
- Designs and conceptualizes systems, tools, and materials necessary for RSBSA registration and updating; and
- Performs other duties/related tasks that may be deemed necessary by the RSBSA-NPSC and National Technical Working Group (NTWG).

#### **DA CO – Information and Communications Technology Service (ICTS)**

- Identifies existing agri-fishery registry databases that must be integrated and/or harmonized with the RSBSA for the achievement of a complete and centralized agri-fishery registry;
- Formulates guidelines and procedures for the harmonization of beneficiary lists per banner program to identify verified active farmers and fishers, subject to the approval of the RSBSA-NPSC;
- Coordinates with concerned agencies and offices and consolidate relevant information, data, or list that may be useful for the harmonization of databases and the establishment of a centralized database;
- Creates and maintain different dashboards related to RSBSA;
- Performs other duties/related tasks that may be deemed necessary by the RSBSA-NPSC and NTWG.

#### **DA CO – Program Monitoring Service (PMS)**

- Institutionalizes the use of RSBSA Reference Number (RSBSAPP-generated reference number) as the official and unique identification of each DA stakeholder and the collection of a standard data set requirement necessary for monitoring DA interventions, programs, projects, and activities;
- Identifies existing interventions monitoring systems that must be integrated for a harmonized data collection and monitoring;
- Designs, develops, and maintains a system enumerating the interventions received and participated in by each RSBSA registrant; and
- Ensure that all RSBSA registrants are issued with DA Interventions Monitoring Card to be presented as identification card in receiving or participating in any DA program.

#### **DA CO – Data Protection Officer (DPO)**

- Performs the duties and responsibilities provided for under National Privacy Commission (NPC) Advisory No. 2017-01;
- Monitors and ensures the compliance of all RSBSA-related systems to the Data Privacy Act of 2012; and
- Coordinates with Regional Compliance Officers for Privacy (COP) as regards all RSBSA data privacy matters in their respective regions.

#### **DA RFO – Compliance Officer for Privacy (COP)**

- Performs the duties and responsibilities provided for under National Privacy Commission (NPC) Advisory No. 2017-01;
- Assists the Data Protection Officer in monitoring and ensuring the compliance of RSBSA-Related systems to the Data Privacy Act of 2012 within their respective regions;



#### **DA RFO – Regional Executive Director (RED)**

- The DA-Regional Field Offices (DA-RFOs) shall be primarily and directly responsible for implementing the program in their respective regions. For this purpose, the Regional Executive Director (RED) shall create a Regional Program Management Office (RPMO) and designate a Permanent and Alternate RSBSA Focal Person who will oversee the implementation of the RSBSA updating at the regional level.

#### **DA RFO – Field Operations Division (FOD) and Planning, Monitoring and Evaluation Division (PMED)**

- Oversees the execution of guidelines issued by the NPMO;
- Monitors the implementation of RSBSA at the municipal level; and
- Coordinates with LGUs and other agencies involved in the RSBSA registration and updating.

#### **DA RFO – Information and Communications Technology Unit (ICTU)**

- Leads the regional RSBSAPP encoding and administration;
- Ensures data is up-to-date and of quality, regularly exercising efforts to reconcile detected probable duplicates and resolve erroneous data; and
- Documents all activities involved and related to the encoding of records.

### **THE DATA PRIVACY ACT**

Republic Act No. 10173, also known as the Data Privacy Act of 2012 (DPA), aims to protect and ensure the security of personal data in information and communications systems both in the government and the private sector.

The DPA ensures that entities or organizations processing personal data establish policies, and implement measures and procedures that guarantee the safety and security of personal data under their control or custody, thereby upholding every individual's data privacy rights. A personal information controller (PIC) or personal information processor (PIP) is instructed to implement reasonable and appropriate measures to protect personal data against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration, and integrity breach.

## **II. INTRODUCTION**

The Registry System for Basic Sectors in Agriculture (RSBSA) respects and values the data privacy rights of its personnel and beneficiaries, specifically the farmers and fisherfolk, and ensures that all personal data collected within the registry system is processed in adherence to the DPA's general principles of transparency, legitimate purpose, and proportionality.

This Privacy Manual is created as a set of protocols that must be observed and followed all throughout the information lifecycle (i.e. collection to destruction), especially in addressing concerns pertaining to the sharing of data with other agencies or individuals who seek to collaborate with the RSBSA of the DA in the implementation of projects and/or in the creation of policies involving farmers and fisherfolks.

Moreover, this Manual serves as a handbook governing the protection of personal data and the rights of the data subjects involved in the processes of the RSBSA, in accordance with the DPA and its Implementing Rules and Regulations (IRR).



### III. DEFINITION OF TERMS

For purposes of this Manual, the following terms are defined as follows:

1. **(DA) Attached Agencies and/or Corporation** - refers to those with attachment or lateral relationship with the DA for purposes of policy and program coordination. The agencies attached to DA shall continue to operate and function in accordance with their respective charters, laws or orders creating them, except as otherwise provided in E.O. 292.
2. **(DA) Bureaus** - refers to any principal subdivision of the DA performing a single major function or closely related functions. Specifically, the DA has the following bureaus:
  - a. Agricultural Training Institute (ATI);
  - b. Bureau of Agricultural Fisheries and Engineering (BAFE);
  - c. Bureau of Agricultural Research (BAR);
  - d. Bureau of Agriculture and Fisheries Standards (BAFS);
  - e. Bureau of Animal Industry (BAI);
  - f. Bureau of Fisheries and Aquatic Resources (BFAR);
  - g. Bureau of Plant Industry (BPI);
  - h. Bureau of Soils and Water Management (BSWM); and
  - i. Philippine Rubber Research Institute (PRRI).
3. **Consent of Data Subject** - refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of personal information about and/or relating to him or her. The consent shall be evidenced by written, electronic, or recorded means.
4. **Compliance Officer for Privacy (COP)** - refers to an individual or individuals who shall perform some of the functions of a DPO as provided in NPC Advisory No. 2017-01, and any other issuance as may be issued by the NPC. Specific duties and responsibilities of the COP are provided for under S.O. No. 422, series of 2022, or any other Special Order as may hereafter be issued by the DA.
5. **Data Subject** - refers to an individual whose personal, sensitive personal or privileged information is processed as defined in Section III(17) hereunder. It may refer to individuals inside or outside this organization (i.e. officers, employees, consultants, and clients).
6. **Department of Agriculture (DA)** - is the executive department of the Philippine government responsible for the promotion of agriculture and fisheries development and growth. It pushes for increased food sufficiency as an effort to ensure food availability, accessibility, and affordability.
7. **Filing System** - refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.
8. **Information and Communications System** - refers to a system for generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or which data is recorded, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data, electronic message, or electronic document.



9. **City/Municipal Agriculturist Office (C/MAO)** - refers to the office in-charge of employing and managing programs and activities relative to agriculture and fisheries of the city/municipality.

10. **National Privacy Commission (NPC)** - is the agency responsible to ensure compliance with international standards set for data protection of the country. It is the government's arm which ensures that the involved bodies remain in full control of its processed personal information in this digital age. It safeguards the rights of the data subject while ensuring the free flow of information for innovation, growth, and national development.

11. **Network Detection and Response (NDR) Tool and the Network Firewall (FW) Appliance** - are tools that provide network security capabilities needed by the Department for protecting its hosted systems. These greatly reduce the attack surface by identifying and allowing access to authorized applications and websites only and providing network-level protection for vulnerabilities. Further, it will also provide advanced anti-malware capabilities and secure connectivity via remote access. The NDR and Network FW Appliance permit to counter-attack the suspicious or malevolent traffic and threats.

12. **Personal Information (PI)** - 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.

13. **Personal Information Controller (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. In this case, the PIC is the DA.

14. **Personal Information Processor (PIP)** - refers to any natural or juridical person qualified to act as such under the DPA to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

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

16. **Registry System for Basic Sectors in Agriculture (RSBSA)** - is the electronic compilation or database of basic information on farmers, farm laborers, and fisherfolk who are the target beneficiaries of agriculture-related programs and services.

17. **RSBSAPP for LGU (RSBSAPP-LGU)** - is a version of the RSBSAPP specifically designed for utilization of capable Local Government Units (LGU) to facilitate the registration of farmers in their local jurisdiction in support of the updating of the Registry System for Basic Sectors in Agriculture (RSBSA).

18. **RSBSA Profiling Platform (RSBSAPP)** [Formerly called Farmers and Fisherfolk Registry System (FFRS)] - refers to an online system used to facilitate the registration of farmers in support of the updating of the RSBSA.

19. **Registry System for Basic Sectors in Agriculture - Project Management Office (RSBSA-PMO)** - refers to the office composed of the RABSA-NPMO, ICTS, and DA RFOs.



20. **(DA) Regional Field Offices (RFOs)** - the regional branch of the Department that facilitates and supervises the formulation and execution of policies, plans, and programs of the DA within its regional jurisdiction. Each Regional Office headed by the Regional Executive Director (RED), shall have the following duties and responsibilities, within its administrative regions:

- a. Provide efficient and effective frontline services to the people;
- b. Implement and enforce in its area the laws and policies, plans, programs, projects, rules, and regulations issued by the Department including plant and animal quarantine laws, rules and regulations;
- c. Coordinate with regional offices of other departments, offices and agencies in the region;
- d. Coordinate with local government units; and
- e. Perform such other functions as may be provided by law or assigned appropriately by the Secretary.

21. **Sensitive Personal Information (SPI)** - refers to personal information:

- a. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- b. 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;
- c. 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
- d. Specifically established by an executive order or an act of Congress to be kept classified.

22. **Valueless Records** - refer to all records that have reached the prescribed retention periods and outlived its usefulness to the RSBSA, or the DA as a whole.

#### IV. SCOPE AND LIMITATIONS

This Manual shall serve as an internal guide for the personnel and staff of the RSBSA-National Program Management Office, its regional implementing units, and different DA attached agencies and corporations as well as its bureaus, and other stakeholders, regardless of the type of employment or contractual arrangement, requiring the processing of personal data of farmers and fisherfolk with respect to the RSBSA.

This Manual covers the treatment of all personal data that the RSBSA holds.

#### V. PROCESSING OF PERSONAL DATA

##### A. DATA PRIVACY PRINCIPLES

1. The RSBSA-PMO abides by the following principles in processing all personal data:



- (1) **Transparency.** The data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of the personal information controller, his or her rights as a data subject, and how these can be exercised. Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.
- (2) **Legitimate purpose.** The processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy.
- (3) **Proportionality.** The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose. Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

## B. COLLECTION

1. The following PI and SPI are collected from farmers and fisherfolk:
  - a. Personal Information
    - (1) Full Name
    - (2) Sex
    - (3) Address
    - (4) Date of Birth (*SPI*)
    - (5) Place of Birth
    - (6) Mother's maiden name
    - (7) MobileNumber
    - (8) Religion (*SPI*)
    - (9) Highest Formal Education (*SPI*)
    - (10) Civil Status (*SPI*)
    - (11) Name of Spouse if married
    - (12) Affiliations (i.e. Farmer Cooperative, 4Ps, IP, PWD)
  - b. Farm Profile
    - (1) Main Agricultural Livelihood (farmer/farm worker/fisher)
    - (2) Farming and fishing activities involved
    - (3) Gross Annual Income (farming and non-farming)
    - (4) Number of farm parcels
    - (5) Agrarian Reform Beneficiary
    - (6) Farm Land Description (for farm owners/tillers)
    - (7) Location
    - (8) Total farm area (in hectares)
    - (9) Proof of ownership
    - (10) Type of ownership (registered owner/tenant, tenant/lessee/others)
    - (11) Crop/Commodity
    - (12) Size per crop/commodity
    - (13) No. of heads (for livestock and poultry)
    - (14) Farm type (irrigated/rainfed upland/rainfed lowland)
    - (15) Practice of Organic Agriculture
2. The RSBSA-hired enumerators will collect such personal data through the accomplished RSBSA Enrollment Form (**Annex A**) and the required attached documents (**Annex B**). The RSBSA Enrollment Form contains a Consent Form and Data Privacy Notice (see Figure 1 below) at the back portion for the data subjects to certify the indicated data are true and correct and that they permit



the data collection for the purposes of documentation, planning, reporting, and implementation of agri-fishery related interventions.

I hereby declare that all information indicated in this form are true, correct and complete, and that they may be used by the Department of Agriculture for the purposes of registration to the RSBSA and other legitimate interests of the Department pursuant to its mandates. I am fully aware that I can be held liable for any misdeclaration or intentional omission made herein pursuant to applicable laws and regulations.

Furthermore, I hereby give consent to the Department of Agriculture to conduct validation activities on my declared farm parcels through the RSBSA Georeferencing Activity.

DATE	PRINTED NAME OF REGISTRANT	SIGNATURE / THUMBMARK
------	----------------------------	-----------------------

VERIFIED TRUE AND CORRECT BY:

SIGNATURE ABOVE PRINTED NAME / DATE Barangay Chairperson / ICC/IPS Leader/Elder (IPs) / C/Mun Veterinarian (Livestock) / Mill District Officer (Sugarcane) / C/MARO (ARBs)	SIGNATURE ABOVE PRINTED NAME / DATE City/Municipal Agri-Fishery Council (C/MAFC) Chairperson	SIGNATURE ABOVE PRINTED NAME / DATE City/Municipal Agriculturist (C/MA) required	SIGNATURE ABOVE PRINTED NAME / DATE Enumerator (if administered) required
---	---	---	--

**DATA PRIVACY NOTICE**

The Department of Agriculture (DA) commits to uphold your rights to privacy as a data subject under the Data Privacy Act of 2012 (DPA). In this regard, the DA shall strictly implement controls and measures compliant to the DPA, its IRR, and the Circulars issued by the National Privacy Commission. All personal information collected through this form shall be used for purposes of documentation, planning, and policy-making, reporting and other connected processes in availing of agri-fishery related interventions. Your information is retained for the duration necessary for the aforesaid purposes, complying with applicable laws and regulations. Personal data processed is not shared with any other party, unless such disclosure is allowed under the DPA. As a data subject, you have the right to reasonable access to personal data, correction of inaccuracies, deletion of information, objection to processing, data portability, claim for compensation for harm caused by misuse, and the option to file a complaint with the NPC for violation of privacy rights. For any data privacy-related concerns, you may contact the Data Privacy Officer at: [dpo@da.gov.ph](mailto:dpo@da.gov.ph).

SIGNATURE ABOVE PRINTED NAME / DATE Barangay Chairperson / ICC/IPS Leader/Elder (IPs) / C/Mun Veterinarian (Livestock) / Mill District Officer (Sugarcane) / C/MARO (ARBs)	SIGNATURE ABOVE PRINTED NAME / DATE City/Municipal Agri-Fishery Council (C/MAFC) Chairperson	SIGNATURE ABOVE PRINTED NAME / DATE City/Municipal Agriculturist (C/MA) required	SIGNATURE ABOVE PRINTED NAME / DATE Enumerator (if administered) required
---	---	---	--

**THIS OFFICIAL RSBSA ENROLLMENT FORM IS NOT FOR SALE**

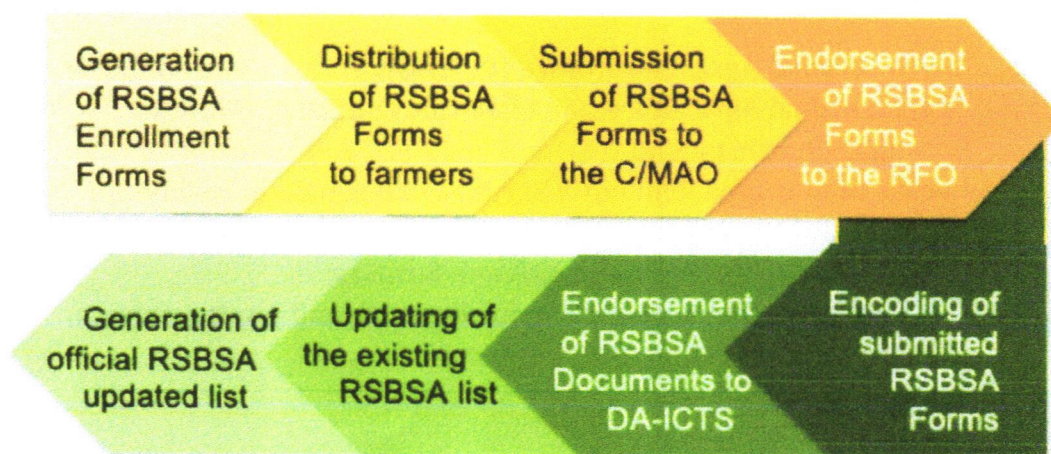
Figure 1. Consent Form and Data Privacy Notice on the RSBSA Enrollment Form

3. The following authorized officials are the certifying authorities of the submitted accomplished RSBSA Enrollment Form and the required attached documents. In consideration of the limited availability of the concerned officials, the C/MAO shall accept submissions duly signed by at least two (2) of the following officials:
- a. City/Municipal Agriculture Office (C/MAO);
  - b. City/Municipal Agriculture and Fisheries Council (C/MAFC);
  - c. Barangay Chairman; and
  - d. In case of non-availability of a Barangay Chairman to certify:
    - (1) C/MARO for Agrarian Reform Beneficiary registrants;
    - (2) Mill District Officer for sugarcane farmers;
    - (3) City/Municipal Veterinarian for livestock and poultry raisers;
    - (4) Tribal Chieftain for IP farmers; and
    - (5) C/MAO for others.
4. Upon submission of the accomplished RSBSA Enrollment Form and compliance with the requirements, the C/MAO shall provide the RSBSA Enrollment Stub to the registrant bearing an LGU-assigned RSBSA reference number and the official DA stamp mark as required security features of the stub as proof of their registration.
5. The C/MAO shall create a masterlist summarizing the accomplished RSBSA enrollment forms being certified and received by their office. The masterlist shall include the following important data fields: (1) Full Name (Last Name, First Name, Middle Name, Extension Name), (2) Reference Number, and (3) Date Received.
6. The C/MAO shall endorse the certified forms to their respective DA-RFOs addressed to the Regional Executive Director (RED) every two (2) weeks, for appropriate action. All official copies of LGU-certified RSBSA Enrollment forms shall be forwarded to DA-RFOs for encoding and safekeeping. The timeline for its safekeeping is specified under E. Storage, Retention and Destruction.



7. RSBSA Regional Encoders shall manually and accurately input the data from accomplished RSBSA Enrollment Forms to the RSBSAPP. They are also tasked to scan and upload in the system the RSBSA Enrollment Forms and the attached documents for filing and electronic documentation purposes.
8. RSBSA-RPMOs shall store all RSBSA attachments in the Network Attached Storage (NAS) procured by each region. RSBSA attachments to be uploaded include (1) a scanned copy of the proof of ownership document (in PDF format), (2) ID photo of the registrants; and (3) a scanned copy of the accomplished RSBSA Enrollment Form (PDF format).
9. All encoded records in the RSBSAPP are under the custody of the Department of Agriculture - Central Office and its respective RFOs, with the DA - Information and Communications Technology Service (DA-ICTS) and its Regional ICT Units as the RSBSA PIPs and the DA Secretary and the Regional Executive Directors as the RSBSA PICs.
10. Know Your Client (KYC) verification process is conducted to verify the personal data of the RSBSA registrants prior to the issuance of the DA Interventions Monitoring Card (DA IMC). The KYC verification process involves the DA-RFOs and accredited Government Financial Institutions and Financial Technology Partners of DA Programs and Projects.

**Flowchart on RSBSA Process**



*Figure 2. DA-RSBSA Updating protocol signed on September 2019*

11. In Local Government Units (LGUs) where the RSBSAPP-LGU has been implemented, its mechanism of implementation embodied under Memorandum Order No. 07, Series of 2024 (**Annex C**) shall be observed.
12. Any substantial change in the data collected or the process of collection shall be embodied in a written documentation shall be approved by the RSBSA-NPMO and/or the Secretary prior execution.

### C. USE

Personal data collected shall be used solely for documentation, planning, reporting, and policy making purposes in availing agri-fishery related interventions.

Processed data shall only be shared to partner agencies for planning, reporting and other legitimate purposes in accordance with the mandate of the DA.



## **D. UPDATING AND CORRECTION**

Personal data shall be accurate and where necessary for declared, specified, and legitimate purpose, kept up to date. Inaccurate or incomplete data shall be rectified, supplemented, destroyed or their further processing restricted.

1. RSBSA registrants who have undergone KYC verification and have been issued with DA IMC, unless otherwise for obvious typographical errors, are allowed to update their static personal information as set under DA Memorandum Order No. 05, Series of 2024.
2. The data subject who wishes to update or correct their RSBSA record shall file a request for updating or correction of data by accomplishing the Updating of Personal Information Slip (**Annex D**), along with necessary documents as proof of the declared updated data.
3. Upon acceptance of the submitted RSBSA Updating Slip, the C/MAO shall administer the verification of correctness and veracity of declared information prior to its endorsement to the respective DA-RFO for encoding. Thereafter the C/MAO shall endorse the accomplished forms to the DA-RFO for encoding. The RSBSA Regional Encoders shall then duly update the data in the RSBSAPP. The accomplished forms as well as the documentary proof shall form part of the records of the data subject.
4. In case of expiration of the validity of RSBSA registration (e.g. deceased, changed occupation to non-farming, etc.), the registrant, or in case of his or her death, the registrant's relative (i.e. legal spouse, parent, child, nearest of kin) with proof of relationship (marriage certificate, birth certificate, Affidavit of Kinship), shall make use of the Updating of Personal Information Slip. The C/MAOs may also submit a letter to the RSBSA-RPMO informing the expiration of the RSBSA record, the reason for expiration, and the proof in support of the reason stated.
5. Once the exclusion of the expired RSBSA record has been approved by the RSBSA, the Regional RSBSAPP administrator shall update the status of the record as inactive in the RSBSAPP. Expired records shall be kept archived within the RSBSAPP for 5 years and will be deleted thereafter if the same remain inactive at the end of the said period.

## **E. STORAGE, RETENTION, AND DESTRUCTION**

The RSBSA-PMO shall ensure that personal data under its custody are protected against any accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. It shall implement appropriate security measures in storing collected personal information.

Personal data, whether in paper or electronic format will be destroyed through secure means that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

Specifically, personal data shall be treated in the following manner:

1. Personal data in paper format and their attachments shall be retained for a period of five (5) years from the moment the same was encoded to the



system and/or digitized. Upon termination of the retention period, the paper forms and their attachments shall be disposed of and destroyed by shredding.

2. Digital/electronic data shall be retained for a period of five (5) years from the time the same are classified as valueless records or its existence is no longer necessary. Upon termination of the retention period, all digital records and their copies shall be deleted from the database and from all storage devices.

## F. ACCESS

Only authorized personnel shall be allowed to access personal data, for any approved purpose, except for those contrary to law, public policy, public order, or morals.

The list of personnel who are authorized to perform designated activities concerning PI and SPI of the data subjects and their access levels are attached as **Annex E**.

## G. DISCLOSURE AND SHARING

All employees and personnel shall maintain the confidentiality and secrecy of all personal data that come to their knowledge and possession, even after resignation, termination of contract, or other contractual relations. Personal data under the custody of the RSBSA-PMO shall be disclosed only pursuant to a lawful purpose, and only to authorized recipients of such data.

Data sharing for the purpose of a public function or provision of a public service shall be covered by a Data Sharing Agreement (DSA).

Data sharing protocols are categorized based on the type of request (i.e. statistics/count, PI/SPI) and operating units (i.e. DA-Operating Units and non-DA Operating Units) requesting data.

TYPE OF DATA	REQUESTING OFFICE/UNIT	
	DA-Operating Units and Bureaus	Attached Agencies, Non-DA (attached agencies, corporations, CSO, LGUs)
Statistics / Count	Send request of specific statistics/count and desired disaggregation of data through official RSBSA email or through submission of RSBSA Request Form	Send request of specific statistics/count and desired disaggregation of data through official RSBSA email or through submission of RSBSA Request Form



TYPE OF DATA	REQUESTING OFFICE/UNIT	
	DA-Operating Units and Bureaus	Attached Agencies, Non-DA (attached agencies, corporations, CSO, LGUs)
<b>Personal and Sensitive Personal Information</b> (any information that can identify a particular individual)	<p>Send a request letter indicating the specific data sets and purposes of the data being requested, and specifying the basis for the request</p> <p>Address letter to: DA Secretary</p> <p>Attention to: Chairperson, TWG on NRSFF</p>	Execute a Memorandum of Understanding (MOU) and Data Sharing Agreement (DSA), as well as a Non-Disclosure Agreement with DA

All data requests with specific data sets shall be coursed through the head of the DA as the PIC. Data requests covering data of a certain region may be coursed through the concerned RSBSA-RPMO. Upon approval of the request, DA-ICTS or RFO-ICTU will process the data sharing.

In cases where PI/SPI is requested, the requesting agency shall submit, in addition to the official letter of request, a proposal for an MOU and DSA with stated provision on the following (Section 9 of NPC Circular No. 202-03, Data Sharing Agreements):

- A. Purpose and lawful basis;
- B. Objectives;
- C. Parties;
- D. Term;
- E. Operational details;
- F. Security;
- G. Data subject's rights;
- H. Retention and disposal; and
- I. Other appropriate stipulations, clauses, terms and conditions.

The MOU and DSA shall be endorsed to the Data Protection Officer (DPO) for review and legal clearance. If the proposal is in order, the request shall be endorsed to the ICTS for processing.

All data sharing documents executed shall be kept in both physical and electronic forms for record purposes and in compliance with Section 10 of NPC Circular No. 2020-03.

## VI. SECURITY MEASURES

The DA RSBSA shall implement reasonable and appropriate physical, technical and organizational measures for the protection of personal data. The security measures aim to maintain the availability, integrity, and confidentiality of personal data and protect them against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.



## A. ORGANIZATIONAL SECURITY MEASURES

### 1. *Data Protection Officer (DPO)*

By virtue of Special Order No. 832, Series of 2023, Atty. Willie Ann M. Angsiy is the designated Data Protection Officer (DPO) of the Department of Agriculture.

### 2. *Duties and Responsibilities of the DPO*

NPC Advisory No. 2017-01 Designation of Data Protection Officers (DPOs) provides for the duties and responsibilities of the DPO, specifically:

- 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:
  - collect information to identify the processing operations, activities, measures, projects, programs, or systems of the PIC or PIP, and maintain a record thereof;
  - analyze and check the compliance of processing activities, including the issuance of security clearances to and compliance by third-party service providers;
  - inform, advise, and issue recommendations to the PIC or PIP;
  - ascertain renewal of accreditations or certifications necessary to maintain the required standards in personal data processing; and
  - 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;
- ensure the conduct of Privacy Impact Assessments relative to activities, measures, projects, programs, or systems of the PIC or PIP;
- 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);
- 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;
- 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;
- 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;
- 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;
- cooperate, coordinate and seek advice of the NPC regarding matters concerning data privacy and security; and
- 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.

### 3. *Compliance Officers for Privacy (COPs)*

Compliance Officers for Privacy shall be designated in each RFO to assist the DPO in overseeing data privacy compliance in their respective jurisdiction and perform such duties as specified in the DPA and related NPC issuances.



#### 4. *Conduct of Training and Seminars*

RSBSA-PMO will organize mandatory training on data privacy and security at least bi-annually. For personnel directly involved in the processing of personal data, the management shall ensure their attendance and participation in relevant training and orientations, as often as necessary.

#### 5. *Privacy Impact Assessment (PIA)*

RSBSA-PMO shall conduct a PIA, at least once every year, relative to all activities, projects, and systems involving the processing of personal data.

#### 6. *Duty of Confidentiality*

All employees with access or involvement with the processing of PI and SPI will be asked to sign a Non-Disclosure Agreement (NDA). All employees with access to personal data shall operate and hold personal data under strict confidentiality if the same is not intended for public disclosure.

#### 7. *Review of Privacy Manual*

This Manual shall be reviewed and evaluated every 15th of December. Privacy and security policies and practices within the organization shall be updated to remain consistent with current data privacy best practices.

### **B. PHYSICAL SECURITY MEASURES**

#### 1. *Format of Personal Data*

Personal data in the custody of the Department may be in digital/electronic format and paper-based/physical.

#### 2. *Storage type and location*

- a. All accomplished RSBSA Enrolment Forms and other related paper-based documents received by DA-RFOs shall be kept secured by the respective RFOs. The documents shall be stored in designated storage areas or kept in locked filing cabinets.
- b. The ICTS is tasked to manage and store all electronic data of the farmer registration in a secure database hosted in a secure infrastructure. The servers may be lodged physically and securely in the DA Data Center or remotely in a Cloud service infrastructure that is compliant with the following:

ISO 27701 - Privacy Information Management

ISO 27018 - Personal Data Protection

ISO 22310 - Security and Resilience

HIPAA - Protected Health Information

ICTS shall perform daily incremental backup and weekly full backup. For on-premise servers, at least two (2) sets of backups are to be maintained, and one (1) set is to be placed off-site or cloud data storage.

- c. All the designated storage areas or the rooms or locations of the filing cabinets where RSBSA data are stored shall be monitored via closed-circuit television (CCTV).
- d. All personnel shall be made aware of the fire response plan and other emergency plans in case of fortuitous events.



3. *Access procedure*

Only authorized personnel shall be allowed to enter or access storage locations, facilities, and devices containing personal data. Other personnel may be granted access upon approval of the Data Protection Officer or Compliance Officer for Privacy of an Access Request (**Annex F**).

Only identified ICTS system developers and database managers are allowed to manage the server and access the database to perform operations, generate reports, and generate analytics on the data.

The staff assigned in the development of reports and analytics will be provided view access only to the datasets.

4. *Monitoring and limitation of access*

Only authorized server administrators shall be allowed to enter the Data Center and manage the servers.

The names of the ICTS staff and their specific roles shall be submitted to the RSBSA-NPMO.

Their specific roles and responsibilities shall be defined in a Special Order.

5. *Design of office space/workstation*

The design of office space and workstations, including the physical arrangement of furniture and equipment, shall provide privacy to anyone processing personal data, taking into consideration the environment and accessibility to the public.

6. *Persons involved in processing, and their duties and responsibilities*

Persons involved in processing shall always maintain confidentiality and integrity of personal data. They are not allowed to use their own gadgets or storage device of any form when entering the data storage room.

7. *Modes of transfer of personal data within the organization or to third parties*

The RSBSA data holdings must always be kept secured. Storing and transfer of these in removable media or workstations is not allowed.

Transfer of data will be done via electronic mail using the official Gov Mail or through uploading to a server using the secure file transfer protocol (SFTP) provided by ICTS. The use of SFTP is always preferred.

8. *Retention and disposal procedure*

Policies and procedures that prevent the mechanical destruction of files and equipment shall be established. The room and workstation used in the processing of personal data shall, as far as practicable, be secured against natural disasters, power disturbances, external access, and other similar threats.

Retention of personal data shall only for as long as necessary, for the fulfillment of the declared specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated.



Personal data shall be disposed of or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

### C. TECHNICAL SECURITY MEASURES

#### 1. *Monitoring for security breaches*

To counter-attack the suspicious or malevolent traffic and threats, a Network Detection and Response (NDR) Tool and the Network Firewall (FW) Appliance shall be in place.

#### 2. *Security features of the software and applications used*

Servers will be configured in a highly secure environment (e.g. DMZ setup, secure cloud infrastructure, and others). The operating system and database software should be configured to comply with minimum security settings such as authorization, and authentication using defined accounts and corresponding passwords.

#### 3. *Process for regularly testing, assessment, and evaluation of the effectiveness of security measures*

A third-party systems audit shall be conducted to determine the vulnerabilities of the applications and databases relative to RSBSA.

Secure Socket Layer (SSL) is employed in the webserver to ensure that all data transmission from the client computer to the server is encrypted.

#### 4. *Encryption, authentication process, and other technical security measures that control and limit access to personal data*

The application system is secured and designed to be accessed using a username, password, and one-time password

Data at rest for the personal profile is encrypted using key management with the encryption algorithm of Advanced Encryption Standard-Counter Mode (AES-CTR) and data in transit through web/https is secured using SSL provided by an internationally recognized signing authority.

## VII. BREACH AND SECURITY INCIDENTS

### A. Data Breach Response Team

A Data Breach Response Team shall be responsible for ensuring immediate action in the event of a security incident or personal data breach. The team shall conduct an initial assessment of the incident or breach in order to ascertain the nature and extent thereof. It shall also execute measures to mitigate the adverse effects of the incident or breach.

Members of the Data Breach Response Team shall be as follows:

1. **Data Protection Officer (DPO)** - manage the Data Breach Response Team;
2. **RSBSA NPMO Member** - oversight representative;
3. **End User** - user representative;
4. **Network Administrator** - experienced in cyber response and defenses including management of the internet and remote access, firewall settings, security updates or patches, and passwords;



5. **Server Administrator** - experienced in troubleshooting of servers, disk storage, virtualization, and cloud services; and in the prevention and detection of server security breaches;
6. **System Administrator / Developer** - experienced in software programming;
7. **Data Privacy Expert** - knowledgeable in legal issuances related to ICT, data privacy, and cybersecurity; and
8. **Digital Forensic Personnel** - knowledgeable in computer forensics and/or cybersecurity.

#### **B. Notification protocol**

The Head of the Data Breach Response Team shall inform the management of the need to notify the NPC and the data subjects affected by the incident or breach within the period prescribed by law. Management may decide to delegate the actual notification to the head of the Data Breach Response Team.

#### **C. Documentation and reporting procedure of security incidents or personal data breach**

A Data Security Incident Report (**Annex G**) shall be accomplished by the personnel first gaining knowledge of the incident or breach encountered. This shall be submitted to the direct supervisor of the personnel as well as to the Data Breach Response Team.

The Data Breach Response Team shall prepare a report containing a detailed documentation of every incident or breach encountered, as well as an annual report, to be submitted to management and the NPC, within the prescribed period.

#### **D. Measures to prevent and minimize the occurrence of breach and security incidents**

The organization shall conduct a Privacy Impact Assessment every December of every year, to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Personnel directly involved in the processing of personal data must attend training and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented in the organization.

#### **E. Procedure for recovery and restoration of personal data**

The organization shall always maintain a backup file for all personal data under its custody. In the event of a security incident or data breach, it shall always compare the backup with the affected file to determine the presence of any inconsistencies or alterations resulting from the incident or breach.

### **VIII. INQUIRIES AND COMPLAINTS**

#### **A. Data Subject's Rights**

The DA RSBSA-PMO recognizes the rights of the data subject in accordance with law, specifically:

- a. Right to reasonable access to his or her personal data being processed by the personal information controller or personal information processor;



- b. Right to dispute the inaccuracy or error in the personal data;
- c. Right to request the suspension, withdrawal, blocking, removal, or destruction of personal data; and
- d. Right to complain and be indemnified for any damages sustained due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of personal data.

## **B. Procedure to Exercise Data Subjects' Rights**

Data subjects may inquire or request for information regarding any matter relating to the processing of personal data under the custody of the organization, including the data privacy and security policies implemented to ensure the protection of their data. They may write to the Department of Agriculture at [info.rsbsa@da.gov.ph](mailto:info.rsbsa@da.gov.ph), copy furnish [dpo@da.gov.ph](mailto:dpo@da.gov.ph), and briefly discuss the inquiry with their contact details for reference.

Complaints shall be filled in three (3) legible printed copies, or sent to [dpo@da.gov.ph](mailto:dpo@da.gov.ph). The Data Protection Officer may instruct the concerned Privacy Focal Person to liaise with the complainant relative to the complaint.

## **IX. SEPARABILITY CLAUSE**

If any clause, sentence, or provision of this Memorandum Order shall be declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.


## **X. REPEALING CLAUSE**

All existing memorandum orders, issuances, rules and regulations, or parts thereof, in conflict with or inconsistent with any provisions of this Order are hereby repealed, modified or amended.

## **XI. EFFECTIVITY**

The provisions of this Manual shall be effective immediately upon approval and shall remain in effect unless revoked in writing.

Done this 5<sup>th</sup> day of July, 2024.

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

*A*



DA-CO-FOS-MO20240619-00002