



**GRAMEEN FOUNDATION USA
PHILIPPINE BRANCH OFFICE**

DATA PROTECTION POLICY

1. Introduction

This Privacy and Data Protection Policy (“**Policy**”) is adopted in compliance with Republic Act No. 10173 or the Data Privacy Act of 2012 (“**DPA**”), its Implementing Rules and Regulations (“**IRR**”), and other relevant policies, including issuances of the National Privacy Commission (“**NPC**”) (collectively, “**PH Privacy Regulations**”). Defined terms used herein will have the same meaning as that provided in PH Privacy Regulations, unless otherwise given a different meaning under this Policy.

Grameen Foundation USA Philippines Branch Office (“**GFUSA-PH**”) respects and values the data privacy rights of all those with whom GFUSA-PH interacts, including employees, partners, contractors, volunteers, board members and its wider network. GFUSA-PH ensures that all Personal Data collected from our employees, partners, contractors, volunteers and any other individual from whom we request Personal Data (“**Data Subjects**”), are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Policy contains information on GFUSA-PH’s data protection and security measures, and may serve as a guide to Data Subjects in exercising one’s rights under the DPA.

This Policy sets GFUSA-PH’s obligations regarding the collection, processing, transfer, storage, and disposal of Personal Data. The procedures and principles set out herein must be followed at all times by GFUSA-PH, its employees, agents, contractors, or other parties working on behalf of GFUSA-PH.

GFUSA-PH is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all Personal Data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. Definition of Terms

Authorized Personnel means anyone with access to Personal Data or Sensitive Personal Data in affiliation with GFUSA-PH.

Personal Data means any personal 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. Personal Data can include, but is not limited to the sample data points in Annex A.

Data Processing means any operation performed upon collected Personal Data by any means including by manual, and/ or digital means including:

1. Organisation, adaptation or alteration of the information or Personal Data;
2. Retrieval, consultation or use of Personal Data;
3. Disclosure of information or data by transmission, dissemination or otherwise making Personal Data available;
4. Alignment, combination, blocking, erasure or destruction of the Personal Data .

Data Subject means a person whose Personal Data is collected, collated, processed or stored by GFUSA-PH. It may refer to employees, partners, contractors, volunteers and members of GFUSA-PH's network.

Sensitive Personal Data means any 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 individual, the disposal of such proceedings, or the sentence of any court in such proceedings; or
3. Issued by government agencies peculiar to an individual which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns.

3. Scope and Limitations

This policy applies to the collection and processing of Personal Data, both in manual and digital formats, including Personal Data held on GFUSA-PH employees, partners, contractors, volunteers and members of GFUSA-PH's network. All personnel of GFUSA-PH, regardless of type of employment or contractual arrangement, must comply with the terms set out in this Data Protection Policy.

4. General Data Privacy Principles

GFUSA-PH shall abide by the General Data Privacy Principles as defined in [Chapter III Section 11](#) of the Data Privacy Act of 2012., and any updates and guidances thereto.

Personal Data must be:

- (a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable after collection, and later processed in a way compatible with such declared, specified and legitimate purposes only;
- (b) Processed fairly and lawfully;
- (c) Accurate, relevant and, where necessary for Data Processing, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;
- (d) Adequate and not excessive in relation to the purposes for which they are collected and processed;
- (e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or for the establishment, exercise or defense of legal claims, or for legitimate business purposes, or as provided by law; and

- (f) Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the data were collected and processed: Provided, That Data collected for other purposes may lie processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: Provided, further, That adequate safeguards are guaranteed by said laws authorizing their processing.

5. Rights of Data Subjects

Under the Philippine Data Privacy Act, data subjects are entitled to the following rights, which GFUSA-PH respects and upholds:

- 5.1. Right to Be Informed: Data Subjects have the right to be informed about how Personal Data is collected, used, stored, shared, and protected. GFUSA-PH will provide information on the purpose of processing and the rights of the data subject before or at the time personal data is collected.
- 5.2. Right to Access: Data Subjects have the right to request information regarding the personal data that GFUSA-PH holds about them. This includes the nature of the data, how it is processed, and the purposes for which it is used. Data Subjects may also request a copy of their Personal Data.
- 5.3. Right to Rectification: Data Subjects have the right to request the correction or updating of personal data that is inaccurate, incomplete, or outdated to ensure that records remain correct and reliable.
- 5.4. Right to Erasure or Blocking: Data Subjects have the right to request the deletion or blocking of Personal Data if it is no longer necessary for the declared purpose, if it has been unlawfully processed, or if consent has been withdrawn.
- 5.5. Right to Object: Data Subjects have the right to object to the processing of Personal Data. This includes processing for direct marketing or profiling. GFUSA-PH will respect the objection unless the processing is required by law or is based on another valid legal ground.
- 5.6. Right to Data Portability: Data Subjects have the right to obtain a copy of their personal data in a structured, commonly used, and machine readable format.
- 5.7. Right to Damages: Data Subjects have the right to claim compensation if they suffer harm due to inaccurate, incomplete, outdated, false, unlawfully obtained, or unauthorized use of Personal Data.
- 5.8. Right to File a Complaint: Data Subjects have the right to file a complaint with the National Privacy Commission if they believe that their data privacy rights have been violated or if they have concerns about the manner in which Personal Data is processed.

6. Processing of Personal Data

- 6.1. GFUSA-PH may only process Personal Data in accordance with a legitimate legal basis. For example, GFUSA-PH may perform the following Personal Data Processing
 - 6.1.1. Workshop / Interview Participants: GFUSA-PH may collect all necessary Personal Data from consenting individuals attending and participating in various GFUSA-PH led or arranged workshops and training activities, including individual subject's full name, contact information, gender and work affiliation. Individuals voluntarily provide this information when they register for a workshop or training and/or when

they sign-in for the event. This Personal Data may be collected electronically or in physical form. Personal Data provided on a physical form is then processed and added to GFUSA-PH secure business cloud computing systems for the purpose of reporting program progress and outcomes of project activities to various funders and donors to GFUSA-PH as well as to track impact of project activities on the subject's respective communities.

- 6.1.2.** Registered Farmers: GFUSA-PH may collect all necessary Personal Data from consenting partner farmers and related cooperatives involved in various GFUSA-PH projects via digital survey tools such as Taroworks, SurveyCTO or ODK applications. Data collected includes farmer demographic profile (Name, Gender, Birthdate, Address), Farm Information (Land area, crops planted, volume of production, GPS location), Farmer Sales Record (Products sold, volume, price received), Trainings (attendance, scores), Cooperative Copra Sales Transactions (such as volume, price, moisture content, deductions, gross and net sales) and Cooperative Staff Demographic Profile (Name, Gender, Role, Contact Details) in order to project registration and market requirement for traceability of products sold and as project requirement for volume projection, training records and communication. Each digital survey tool provides individuals with a privacy notice and obtains written informed consent for processing and using their Personal Data for the purposes outlined herein.
- 6.1.3.** Microfinance Institutions (MFIs): GFUSA-PH may collect all necessary Personal Data from Partner MFIs involved in various GFUSA-PH projects including Personal Data on MFI members (Name, Gender, Birthdate, Contact Details) and MFI Member Loan Transactions (Amount, Due, Date, Frequency) as part of GFUSA-PH's contractual obligations and project requirements for projects with MFI partners and in order to provide credit worthiness analysis when requested. This Personal Data is collected electronically or in physical form. Personal Data provided on a physical form is then processed and added to GFUSA-PH secure business cloud computing systems for the purpose of due diligence, and reporting program progress.
- 6.1.4.** Employment Application and Individual Consultants: GFUSA-PH may collect all necessary Personal Data voluntarily provided by employment applicants or individual subjects that are entering into contracts with GFUSA-PH, including the subject's full name, contact information and Curriculum Vitae / Biodata. Personal Data is collected in order to fairly assess the possible contracting of an applicant. Once contracted, GFUSA-PH retains all necessary Personal Data of an employee and collects additional Personal Data necessary for employment such as their Tax Identification Number (TIN), Social Security, Home Development Mutual Fund and PhilHealth Numbers) in order to comply with government requirements and assure employees receive full benefits. Likewise, GFUSA-PH collects an individual contractor's TIN in order to comply with government withholding tax declaration. Individual consultants are required to fill up GFUSA-PH's Vendor/Consultant Questionnaire and Accreditation (VQA) Form and Vendor/Consultant Electronic Fund Transfer Authorization Form to provide necessary Personal Data for contracting such as their full name, contact information, address, and bank information details for disbursement of contract payment.
- 6.1.5.** Contracts with other Organizations: GFUSA-PH may collect all necessary Personal Data from consenting potential organizational partners or contractors, including the

subject's government registered name, registered address, and names and contact details of responsible partners and a scanned copy of the organization's publicly available registration documents. Consultants are required to fill up GFUSA-PH's Vendor/Consultant Questionnaire and Accreditation (VQA) Form and Vendor/Consultant Electronic Fund Transfer Authorization Form to provide necessary Personal Data for contracting such as their full name, contact information, address, and bank information details for disbursement of contract payment.

6.1.6. Vendors: GFUSA-PH may collect all necessary Personal data from vendors including registered name, registered address, contact details, role and government registration details and documentation. Vendors are required to fill in GFUSA-PH's Vendor/Consultant Questionnaire and Accreditation (VQA) Form and Vendor/Consultant Electronic Fund Transfer Authorization Form either in physical and/or digital form then processed digitally to GFUSA-PH secure business cloud computing systems or to provide necessary Personal Data for contracting such as their full name, contact information, address, and bank information details for disbursement of contract payment.

6.1.7. Volunteers: GFUSA-PH may collect all necessary Personal Data from consenting individuals voluntary GFUSA-PH led or arranged workshops, training activities, technical assistance and support, including individual subject's full name, contact information, gender and work affiliation. Individuals voluntarily provide this information when they register to become a GFUSA-PH volunteer. This Personal Data is collected electronically or in physical form. Personal Data provided on a physical form is then processed and added to GFUSA-PH secure business cloud computing systems for the purpose of reporting program progress and outcomes of project activities to various funders and donors to GFUSA-PH as well as to track impact of project activities on the subject's respective communities.

6.2. Limited Access to Authorized Personnel

All Authorized Personnel shall minimize their processing of Personal Data to the extent reasonably possible to achieve the legitimate business purpose. All Authorized Personnel have the duty to use anonymized data wherever reasonably possible.

All Authorized 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. All Authorized Personnel shall operate and hold Personal Data under strict confidentiality.

Authorized Personnel shall be allowed to access such Personal Data, for the limited purposes compatible with the declared, specified, and legitimate in accordance to the original legal basis for processing. For example, Personal Data related to project activities which includes Personal Data on workshop/interview participants, registered farmers, volunteers and consultants shall be accessible by program staff, while Personal Data related to GFUSA-PH employees shall be accessible by HR staff and the individual's designated manager.

6.3. Disclosure and Sharing

6.3.1. Personal Data under the custody of the GFUSA-PH shall be disclosed to the minimum amount reasonably necessary to achieve the business objective, and only

pursuant to a lawful purpose, and to authorized recipients of such Personal Data in compliance with applicable law.

- 6.3.2. Data sharing agreements must be held with any third party accessing GFUSA-PH Personal Data. Authorized Personnel shall access only data necessary for the performance of assigned duties, comply with GFUSA-PH Data Protection Policy (or their own if substantially similar and in compliance with applicable law), report any incidents or breaches, and support GFUSA-PH in protecting the privacy of Data Subjects. They shall handle Personal Data responsibly ensuring confidentiality, integrity and lawful use.
- 6.3.3. Due Diligence and a Privacy Impact Assessment shall be conducted on each potential third party accessing GFUSA-PH Personal Data.

7. Non-Technical Security Measures

- 7.1. **Data Protection Officer.** The designated Data Protection Officer (DPO) is Sabrina Quaraishi, President and CEO of GFUSA-PH. The Data Protection Officer shall oversee the compliance of GFUSA-PH with the law and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and overseeing the inquiry and complaints procedure.
- 7.2. **Conduct Training.** GFUSA-PH shall hold a mandatory training on data privacy and security at least once a year. For personnel directly involved in the Data Processing, management shall ensure their attendance and participation in relevant training and orientations, as often as necessary
- 7.3. **Conduct Privacy Impact Assessment.** GFUSA-PH shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the Data Processing. It may choose to outsource the conduct of a PIA to a third party.
- 7.4. **Recording and documentation of activities by the DPO.** The DPO shall, or shall delegate to GFUSA-PH staff, to record and document all GFUSA-PH Personal Data collection, processing, transfer, and erasure.
- 7.5. **Duty of Confidentiality.** GFUSA-PH Authorized Personnel will be asked to sign a Non-Disclosure Agreement or some type of contract or agreement with confidentiality obligations with respect to Personal Data. All Authorized Personnel shall operate and hold Personal Data under strict confidentiality if the same is not intended for public disclosure.
- 7.6. **Review of Data Protection Policy.** This policy shall be reviewed and evaluated annually. Privacy and security policies and practices within GFUSA-PH shall be updated to remain consistent with current data privacy best practices.

8. Physical Security Measures

- 8.1. **Format of data.** Personal Data in the custody of GFUSA-PH may be in digital/electronic format and paper-based/physical format. Digital format includes: Text, Photos, Videos, Audio – depending on the needs of the project. Paper based format includes: Records collected individually, or in a group setting
- 8.2. **Storage type and location.**
 - 8.2.1. **Physical.** All Personal Data in paper-based/physical format shall be processed into a secure digital/electronic format by GFUSA-PH. All Personal Data in paper-based/physical format shall be stored in locked filing cabinets in the GFUSA-PH office until they are electronically processed. Then the physical format

shall be destroyed by secure shredding. Digital/electronic files are stored in GFUSA-PH secure business cloud computing systems in multi-factor authentication (“MFA”), password protected computers provided and installed by the GFUSA-PH.

8.2.2. Digital. Digital / electronic files are also stored in MFA password protected cloud-based content management, collaboration, and file sharing tools such as Box folders and Google Drive folders, as well as cloud-based customer relationship management software such as Salesforce, managed and installed by GFUSA-PH, unless specifically specified by the project client / requirements.

8.3. Secure Access.

8.3.1. Physical. Only Authorized Personnel have access to the keys to the locked filing cabinets. Other personnel may be granted access to the office space upon request to the office manager and administrative personnel.

8.3.2. Digital. Digital/electronic files are stored in computers provided by GFUSA-PH that are also securely stored. Digital/electronic files that are also stored in cloud file sharing applications such as Google Drive and Box shall have limited access to authorized personnel. For example, Personal Data related to project activities which includes Data on workshop participants, registered farmers, volunteers and consultants shall be accessible by program staff, while Personal Data related to GFUSA-PH Employees shall be accessible by HR staff and the individual’s designated manager.

8.4. Monitoring and limitation of access. All Authorized Personnel to enter and access the GFUSA-PH lockers must fill out and register via an online tracker. They shall indicate the date, time, duration and purpose of each access. Access to digital/electronic files shall also be limited to access using GFUSA-PH computers and devices.

8.5. Devices. Authorised Personnel are not allowed to bring their own devices, gadgets or storage of any form. Access to Personal Data on digital/electronic files shall be limited via the use of GFUSA-PH installed and owned devices.

8.5.1. Transfers. Transfers of Personal Data via electronic mail shall use a secure email facility with encryption of the data, including any or all attachments. Facsimile technology shall not be used for transmitting documents containing Personal Data.

9. Technical Security Measures

9.1. Security Measures Generally. GFUSA-PH will implement appropriate security measures in storing collected Personal Data, depending on the nature of information, such as but not limited to access by authorized team personnel through password protected accounts, multi-factor authentication, and audit trail for revisions on data. Encryption, authentication process, and other technical security measures that control and limit access to Personal Data must be used at all times.

9.2. Monitoring for security breaches. GFUSA-PH shall use firewall, antivirus and malware detection software to monitor for and prevent security breaches on individual computers.

9.3. Security features of the software/s and application/s used. GFUSA-PH shall review and evaluate software applications before the installation thereof in computers and devices of GFUSA-PH to ensure the compatibility of security features with overall operations.

- 9.4. **Testing.** Regular testing, assessment and evaluation of effectiveness of security measures shall be conducted by the DPO or his/her designee.
- 9.4.1. **Authentication.** Authorized Personnel with access to Personal Data shall verify his or her identity using a secure encrypted link and/or multi-level authentication to access Personal Data.

10.Retention and Disposal.

- 10.1. GFUSA-PH will 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 Data Processing.
- 10.2. GFUSA-PH shall retain the Personal Data of a client so long as there is a lawful basis for holding such data. For example, it may be three (3) years from the end of a project period. Upon expiration of such period, all physical and electronic copies of the Personal Data shall be destroyed and disposed of using secure technology.
- 10.3. GFUSA-PH shall retain the Personal Data of employees, volunteers and consultants for as long as required by Philippine law and the relevant Philippine government agencies (SEC, DOLE, BIR, etc.).
- 10.4. Personal Data will be deleted under the following circumstances: the Data Subject has withdrawn consent to processing; a connected contract has been completed or can no longer be performed; or the data is no longer up to date.

11. Breach and Security Incidents

- 11.1. **Data Breach Response.** The DPO or their designee shall be responsible for ensuring immediate action in the event of a security incident or Personal Data breach. They 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.
- 11.2. **Measures to Prevent and Minimize Occurrence of Breach and Security Incidents.** DPO requires Authorized Personnel to regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of computer networks. Authorized Personnel directly involved in Data Processing must attend training and seminars for capacity building.
- 11.3. **Procedure for Recovery and Restoration of Personal Data.** GFUSA-PH 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.
- 11.4. **Notification Protocol.** In accordance with NPC Circular No. 16-03, upon discovery or reasonable suspicion of a personal data breach, the DPO and the Data Breach Response Team will immediately conduct a preliminary assessment. This assessment determines whether a breach has indeed occurred, the nature and scope of the incident, the personal data that may be involved, the risks or potential harm to individuals, and whether the incident triggers the notification requirements set out under applicable regulations. If the preliminary assessment confirms that a breach has occurred, a full evaluation follows. Notification to the NPC and to affected Data Subjects is required if the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected Data Subjects.

Notifiable data breaches must then be reported to the NPC and to affected Data Subjects within 72 hours from the discovery of a notifiable personal data breach.

11.5. Documentation and Reporting Procedure of Breach or Security Incidents. DPO or their designee shall prepare 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.

12. Inquiries and Complaints. Any Data Subject for whom GFUSA-PH has Personal Data has the right to access, amend, correct or delete any and all Personal Data. A Data Subject has the right to receive Personal Data provided to GFUSA-PH in a “structured, commonly used and machine-readable format.” A Data Subject may lodge a complaint, or request for information regarding any matter relating to the processing of their Personal Data under the custody of GFUSA-PH, including the data privacy and security policies implemented to ensure the protection of their Personal Data by contacting GFUSA’s Data Protection Officer via squaraishi@grameenfoundation.org. GFUSA-PH shall confirm with the complainant its receipt of the complaint and address the concern as soon as possible.

13. Effectivity. The provisions of this Policy are effective this __ day of _____, 2026, until revoked or amended by this GFUSA.

ANNEX A

Types of Personal Data Collected

1. From Workshop/Interview Participants: full name, contact information, gender and work affiliation
2. From Registered Farmers: includes farmer demographic profile (Name, Gender, Birthdate, Address), Farm Information (Land area, crops planted, volume of production, GPS location), Farmer Sales Record (Products sold, volume, price received), Trainings (attendance, scores), Cooperative Copra Sales Transactions (such as volume, price, moisture content, deductions, gross and net sales) and Cooperative Staff Demographic Profile (Name, Gender, Role, Contact Details) in order to project registration and market requirement for traceability of products sold and as project requirement for volume projection, training records and communication.
3. From MFIs: MFI members (Name, Gender, Birthdate, Contact Details) and MFI Member Loan Transactions (Amount, Due, Date, Frequency) as part of GFUSA-PH's project requirements for projects with MFI partners and in order to provide credit worthiness analysis when requested
4. From Employment Applicants and Consultants: full name, contact information and Curriculum Vitae / Biodata, Tax Identification Number (TIN), Social Security, Home Development Mutual Fund and PhilHealth Numbers;
5. From other organizations: government registered name, registered address, and names and contact details of responsible partners and a scanned copy of the organization's publicly available registration documents
6. From Vendors: registered name, registered address, contact details, role and government registration details and documentation
7. From Volunteers: full name, address, other contract information, Curriculum Vitae / Biodata, Medical Release and Emergency Contacts, Scanned copy of Philhealth ID for insurance, Banking Information for travel expenses, Volunteer Reference

This Annex A is general and for example only. Data Subjects should receive notice forms addressing personal data collection where consent is the basis for collection and processing.