Mindanao Peacebuilding Institute Foundation, Incorporated

Privacy and Data Protection Manual

November 23, 2018

Mindanao Peacebuilding Institute Foundation, Inc.
Privacy and Data Protection Manual

Table of Contents

Mindanao Peacebuilding Institute Foundation, Inc.
Privacy and Data Protection Manual

Introduction

This Privacy and Data Protection Manual 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. The Mindanao Peacebuilding Institute Foundation, Inc. (MPI) respects and values the data privacy rights of all those with whom MPI interacts, including participants, alumni, staff, volunteers, board members and its wider network. MPI ensures that all personal data collected from our participants, alumni, staff, volunteers and any other individual from whom we request personal information, are processed in adherence to the general principles of transparency, legitimate purpose, and proportionality.

This Manual shall inform the reader of our data protection and security measures, and may serve as a guide in exercising one's rights under the DPA.

Definition of Terms

Consent of the data subject refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so.

Data sharing is the disclosure or transfer to a third party of personal data under the custody of a personal information controller or personal information processor. In the case of the latter, such disclosure or transfer must have been upon the instructions of the personal information controller concerned. The term excludes outsourcing, or the disclosure or transfer of personal data by a personal information controller to a personal information processor.

Data Subject refers to an individual whose personal, sensitive personal or privileged information is processed by the Mindanao Peacebuilding Institute Foundation, Inc. It may refer to officers, employees, facilitators, training participants, alumni, volunteers and members of MPI's network.

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 individual is readily accessible.

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 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.

Personal data breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

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

Personal information controller refers to a person or organization (in this case MPI) 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.

Personal information processor refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

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.

Scope and Limitations

This policy applies to the keeping and processing of personal data, both in manual form and on computer, including personal data held on MPI staff, officers, training participants and alumni.

All personnel of MPI, regardless of the type of employment or contractual arrangement, must comply with the terms set out in this Privacy and Data Protection Manual.

General Data Privacy Principles

MPI shall abide by the General Data Privacy Principles as defined in Chapter III Section 11 of the Data Privacy Act of 2012.

Personal information 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 purposes for which it is to be used for the processing of personal information, 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 fulfilment 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 personal information collected for other purposes may be 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.

Processing of Personal Data

A. Data Collection and Use

1. Website Registration: When registering for the MPI website as an alumna/us or part of the MPI network, MPI requests the name, organization, email, relationship to MPI and general location in order to understand who is connecting with MPI and to help alumni connect with one another. MPI also request alumni to indicate the year(s) and course(s) they took in order to give access to handouts and to assist in connecting alumni with one another. This data is monitored and controlled by the website administrator.
2. MPI Occasional Newsletter: MPI requests a subscriber's name, email organization, country and position to enable the subscriber to receive the email and to help MPI understand who is interested in hearing from MPI.
3. Application for MPI Trainings: Individuals applying for an MPI training program or activity will be asked to submit information appropriate to the training and for acceptance and placement. Details on what information is collected and why can vary depending on the training, but generally include their full name, address, email address, phone number, education and work background. Other data collected may include sex, dietary needs, language ability and other physical concerns in order to fully address participants needs during the training.
4. MPI Alumni Newsletter: When individuals register for a training programs, that information is utilized to include individuals in MPI's alumni mailing list. The information that is included in the mailing lists consists of one's name, email address, organization, position, country and year in which you participated in the Annual Peacebuilding Training or other training. This information also allows MPI to segment the mailing lists and to know what organizations are represented and by whom.
5. Email Inquiries: When visitors to the website use our "Contact Us" from, MPI collects the email address, name and the information provided in the inquiry in order to respond to the request.
6. Employment Application and Contracts: MPI collects all necessary information from those applying for employment or entering into contracts with the institute, including an applicant's full name and contact information as well as an applicant's Curriculum Vitae. Such information is collected in order to make a fair decision on hiring or retaining a contract. Once hired, MPI retains all necessary information of an employee and collects any additional information, such as a government issued IDs (Tax Identification Number, Social Security, PhilHealth) in order to comply with government requirements and assure the employee receives full benefits.
7. Board of Trustees: MPI request the full name, address, phone/mobile phone, email address and background information of those candidates for and members of MPI's Board of Trustees. Initial information is collected in order for existing board members to select new members. Once serving as a board member, the information is utilized for communication purposes and for complying with government requirements related to the makeup of the Board of Trustees. Basic information is also utilized for public information regarding the makeup of the Board of Trustees.

B. Storage, Retention and Destruction of Data

The Mindanao Peacebuilding Institute 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 processing. MPI will implement appropriate security measures in storing collected personal information, depending on the nature of the information.

In the absence of any legal requirements, personal data will only be retained as long as necessary for the purpose of processing. Data will be deleted under the following circumstances:

- the data subject has withdrawn consent to processing;
- a contract has been performed or cannot be performed anymore; or
- the data is no longer up to date.

MPI adapts the following specific data retention policies with respect to its constituents:

1. Training Applicants: MPI will retain the data submitted by applicants for any training conducted by the Institute for no more than five years, unless the individual is accepted into the training program or has chosen to reapply. For those individuals reapplying for a training program, MPI will ensure that her/his data is up-to-date and accurate.
2. Training Participants: MPI will retain the complete data of training participants for no more than seven years after completion of the training, unless the individual applies for another training within the period, with the exception of financial records (e.g., invoices), which must be retained for a period of 10 years. For those individuals applying for another training program, MPI will ensure that her/his data is up-to-date and accurate.
3. MPI Alumni: MPI retains the minimum information (email address, organization, position, country) from the training participants' applications to maintain a list of MPI alumni in order to include the alumni in communication directed to them and to achieve MPI's objective to "connect people from diverse sectors to build a critical mass of peacebuilders to promote justpeace." Data will be deleted/destroyed if the data subject (alumna/us) has withdrawn consent to processing or the data is no longer up to date. Any other retained information will be anonymized of aggregated for statistical purposes only.
4. MPI Employees, Volunteers, Contracted Services and Board of Trustees: MPI retains the personal data of employees, volunteers, those with whom MPI enters into contracted services, and the members of the Board of Trustees for as long as required by Philippine law and the relevant Philippine government agencies (SEC, DOLE, BIR, etc.) only and not beyond. Any information retained beyond this period is anonymized or aggregated.
5. Website and Newsletter Data: Personal Data on the website is backed up monthly but only retained for three months, after which the backup data is deleted. Data of those who have unsubscribed from or who have invalid email addresses for the MPI mailing lists will be removed within three months (email data is retained to prevent inadvertent resubscription without consent).

C. Access

The Mindanao Peacebuilding Institute Foundation, Inc., recognizes the sensitive and confidential nature of the personal data under its responsibility. Only the constituent and the authorized representatives of MPI shall be allowed to directly access such personal data, for any purpose, except for those contrary to Philippine law or public policy or international law or policy that is not superseded by Philippine laws or public policy. Please see MPI's Access Control Policy for further details.

D. Disclosure and Sharing

All employees and personnel of the Mindanao Peacebuilding Institute 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 MPI shall be disclosed only pursuant to a lawful purpose, and to authorized recipients of such data.

With respect to MPI's trainings, the Institute shares the minimal information necessary with course facilitators in order for them to properly conduct the courses to which they are assigned (e.g., English proficiency). In addition, MPI shared the necessary information with the host venue to accommodate the participants, particularly name and sex for room assignments. Other personal data is given in aggregate format, such as dietary restrictions.

MPI utilizes third-party services in the processing of data collected through the MPI website (www.mpiasia.net). MPI uses Google Analytics to collect standard internet log information and details of visitor behavior patterns. MPI uses MailChimp for sending out a newsletter to its alumni. The data collected includes name, email address, organization, country and MPI training attended. Please see MailChimp's Legal Policies with respect to their own privacy policies and use of data.

Security Measures

A. Organization Security Measures

1. Data Protection Officer (DPO): The designated Data Protection Officer is Mr. Frederick Goddard, who is concurrently serving as the Technical and Institutional Capacity Building Officer of the Mindanao Peacebuilding Institute Foundation, Inc.
2. Functions of the DPO: The Data Protection Officer shall oversee the compliance of MPI with the DPA, its IRR, and other related policies, including the conduct of a Privacy Impact Assessment, implementation of security measures, security incident and data breach protocol, and the inquiry and complaints procedure.
3. Conduct of trainings or seminars: MPI shall conduct an internal mandatory training or require its staff to attend an external training on data privacy and security at least once a year. For personnel directly involved in the processing of personal data, management shall ensure their attendance and participation in relevant trainings and orientations when available.
4. Privacy Impact Assessment (PIA): MPI shall conduct a Privacy Impact Assessment (PIA) relative to all activities, projects and systems involving the processing of personal data. MPI may choose to outsource the conduct a PIA to a third party.
5. Recording and documentation: MPI shall record and document all activities carried out by the DPO or MPI itself to ensure compliance with the DPA, its IRR and other relevant policies.
6. Duty of Confidentiality: All MPI employees, personnel and volunteers will be asked to sign a Non-Disclosure Agreement. 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 annually. Privacy and security policies and practices within MPI shall be updated to remain consistent with current data privacy best practices.

B. Physical Security Measures

1. Format of data to be collected: Personal data in the custody of MPI may be in digital/electronic format and/or paper-based/physical format.
2. Storage type and location: All personal data being processed by MPI shall be stored in locked filing cabinets in the Admin/Finance Office. Digital/electronic files are stored in computers provided by MPI that are also securely stored.
3. Access procedure of MPI personnel: The Admin and Finance Officer are designated to monitor access to their office and to the locked personal data file cabinets, each of whom has a key to the office. Access to the file cabinet for internal personal data files (i.e., human resources) is limited to the Admin Officer, the Director and the Data Protection Officer. Access to personal data files of training participants is limited to the Peacebuilding Training Program Officer, the Director and the Data Protection Officer. Other personnel may be granted access to the file cabinets upon filing of an access request form with the Data Protection Officer and the approval of both the DPO and the Director.

4. Monitoring and limitation of access to room or facility: All personnel authorized to access the data must fill out the logbook placed on the respective file cabinet. They shall indicate the date, time, duration and purpose of each access.
5. Design of office space/work station: Computers are positioned with considerable spaces between them and in a position to maintain privacy and protect the processing of personal data.
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 utilize their own cell phone, tablet, laptop, camera or any other personal electronic or other type of storage device when accessing personal data files or materials.
7. Retention and disposal procedure: As outlined above, In the absence of any legal requirements, personal data will only be retained as long as necessary for the purpose of processing. For details on MPI's retention policy, see section B under *Processing of Personal Data*: *Storage, Retention and Destruction of Data*. Upon expiration of the outlined periods, all physical and electronic copies of the personal data shall be destroyed and disposed of using secure procedures—shredding of hard copies and a secure erasing tool such as *Cipher* or *Erase* of electronic copies.

C. Technical Security Measures

1. Monitoring for security breaches: MPI shall use firewalls, antivirus software and malware detection software to monitor for and prevent security breaches on individual computers.
2. Security features of the software/s and application/s used: MPI shall review and evaluate software applications before installation on MPI computers and other devices to ensure the compatibility of security features with overall operations.
3. Modes of transfer or exchange of personal data within the organization or to third parties: Transfers of personal data via electronic mail or any other digital procedure shall be done through secure technology with encryption of the data, including any or all attachments. If the personal data is sent as an attachment, the attachment shall be encrypted. If the personal data is sent in the body of the email, the email itself shall be encrypted. Facsimile (FAX) technology shall not be used for transmitting documents containing personal data.
4. Process for regularly testing, assessment and evaluation of effectiveness of security measures: MPI shall review security policies and conduct regular security testing within the Institute and for the MPI website on a regular schedule. MPI uses Beyond Security for website testing, which is done on a weekly basis.
5. Encryption, authentication process, and other technical security measures: Each personnel with access to personal data shall verify his or her identity using a secure encrypted link and multi-level authentication.

Breach and Security Incidents

A. Data Breach Response Team

A Data Breach Response Team comprising the Data Protection Officer, the Director and the Admin Officer 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.

B. Measures to prevent and minimize occurrence of breach and security incidents

MPI shall regularly conduct a Privacy Impact Assessment to identify risks in the processing system and monitor for security breaches and vulnerability scanning of its computer network and website. Personnel directly involved in the processing of personal data must attend trainings and seminars for capacity building. There must also be a periodic review of policies and procedures being implemented by MPI.

C. Procedure for recovery and restoration of personal data

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

D. Notification protocol

The Data Protection Officer, along with the Director, shall inform the Board of Trustees of the need to notify the NPC and the data subjects affected by the incident or breach within 72 hours. The BoT may decide to delegate the actual notification to the head of the Data Breach Response Team.

E. Documentation and reporting procedure of security incidents or a personal data breach

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

Inquiries and Complaints

Any data subject for whom MPI has personal data has the right to access, amend, correct or delete any and all personal information. Those registered for the MPI website may update, make private or delete their profile at any time. Those subscribed to MPI's electronic mailing lists may access and amend their personal information or unsubscribe completely. A data subject may also request that any personal data amended, corrected or erased by completing the Correction or Erasure Form online or through a physical form.

A data subject has the right to receive personal information provided to MPI in a "in a structured, commonly used and machine-readable format." Data subjects may inquire or request for information regarding any matter relating to the processing of their personal data under the custody of the MPI, including the data privacy and security policies implemented to ensure the protection of their personal data. They may download or request an Inquiry Form from MPI and submit it to mpi@mpiasia.net or mail it to MPI or complete the online Inquiry Form.

Complaints shall be filed in three (3) printed copies, submitted through an online complaint form through the MPI website or sent to complaints@mpiasia.net. MPI shall confirm with the complainant its receipt of the complaint and address the concern as soon as possible.

Effectivity

The provisions of this Manual are effective this 23rd day of November 2018, until revoked or amended by the Mindanao Peacebuilding Institute Foundation, Inc., through a Board Resolution.

Annexes

1. Access Control Policy
2. Access Request Form
3. Sample Consent Form*
4. Inquiry Form
5. Non-disclosure Agreement
6. Privacy Notice
7. Request for Correction or Erasure

* MPI utilizes different consent forms, depending on the activity. The consent forms included here are samples that represent MPI's approach to obtaining consent.