Data protection policy

1. Introduction

Darshna Mahila Kalyan Samiti, processes personal data. This policy concerns the processing of personal data of different categories of identifiable persons such as employs, stakeholders, beneficiaries, partners. DMKS understand the importance of personal data and always carefully considers the protection of personal data during the different personal data processing operation. DMKS, compliance with data protection legislation is the basis for a relationship of trust between DMKS & it's staff, partners & donors. DMKS takes the protection of personal data very seriously & the data protection policy assign responsibility for data protection and authorize protocol for DMKS staff.

2. Objectives

DMKS data protection policy refers to our commitment to treat information of employees, beneficiaries, stakeholders & donors with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

The objectives of this policy are as follow:

1. To create uniform framework and effective standard for the protection and use of personal data within DMKS.
2. Follow "do-not-harm-principal" in line with the core humanitarian standard on quality and accountability given from funding agency.
3. To follow, compliance with data protection legislation is the basis for a relationship of trust.
4. to safeguard the fundamental rights and freedoms of Data Subjects, in particular, their right to the protection of Personal Data, and to ensure an adequate level of protection of Personal Data processed by DMKS through general organisational measures and the allocation of responsibilities.

3. Scope

This policy applies to all staff within the organization (Permanent staff, Temporary staff, Volunteers, Stake holders, Partners, Beneficiaries, Project Participants, Supplier). Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4. Definitions

4.1. Data Controller

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determine the purpose and means of the processing of personal data. Where the purposes and means such processing and determined by Board Members of DMKS.

4.2. Deletion & Anonymization

Personal data may only be stored for as long as it's necessary for the purpose for which the data is being processed this means that personal data must be deleted or anonymized as soon as the purpose of its processing has been fulfilled or otherwise lapse.

4.3. Consent

Consent any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action.

4.4. Biometric Data

Biometric data is Personal Data resulting from specific technological processing relating to the physical, physiological, or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

4.5. Data Protection Officer

The Data Protection Officer is a function foreseen by applicable mandatory law to support the due application of data protection law in the context of the operations of a Head Office.

4.6. Data Subject

Data subject any natural person who is identified in or identifiable based on personal data, like e.g. Donors, Employees, Beneficiaries, Project Participants, Stakeholders.

4.7. Personal Data

Personal data means any data related to an individual who can be identified form that data; from that data and other information; or by means reasonably likely to be used related to that data. Personal data include bio graphical data (bio-data) such as Name, Sex, Martial Status, Date & Place of Birth, Country of Origin, individual registration number, religion and ethnicity, bio-metric data such as photograph, fingerprint, as well as any expression of opinion about the individuals, such as assessment of the status and/or specific needs.

4.8. Processing of Personal data

Processing of Personal data means any operation, or set of operation, automatic or not, which is performed on personal data, including but not limited to the collection, recording, organization, structuring, adoption, or alteration, retrieval, consultation, use, transfer (which is computerized, oral or written form), dissemination or otherwise making available, correction or destruction.

4.9. Processing Restriction

A processing restriction is the marking of stored personal data with the aim of limiting its future process.

4.10. Employee

Any employee of Darshna Mahila Kalyan Samiti.

4.11. Head Office

Darshna Mahila Kalyan Samiti's Head Office operations at Chhatarpur (M.P) India.

4.12. Profiling

Profiling means any form of automatic processing of personal data consisting of the use of personal data to evaluate certain personal aspect relating to a natural person, in particular to analyse or predict aspect concerning the natural person's performance at work, economic situation, health, personal performance, interest, reliability, behaviour or movements.

4.13. Darshna Mahila Kalyan Samiti or DMKS

Darshna Mahila Kalyan Samiti, Chhatarpur, registered with the Registered Society, Registration no.SC/2532/ 26 may 1999, Registered under 12AA of .I.T.Act.1976, Registered under AA/GWL/80G/35/12/2007-08, Registered under FCRA Act 1976.

4.14. Third Party

Third Party means a natural or legal person, public authority, agency, or other body other than the Data Subject, the Controller, the Data Processer, and other persons who have direct authorisation from the Controller or the Data Processor to process Personal Data.

5. Data Protection: Organisation Structure

5.1. General Organisation

The overall responsibility for Data Protection lies with the Board members and coordinator from each project. The Privacy Officer support them in performing their duties.

5.2. Local Responsibility

DMKS Management is responsible for complying with data privacy laws and regulations pertaining to its Office. In addition, it must ensure that managers, & Employees that process Personal Data for which DMKS is responsible or is acting as Data Processor, within the meaning of the GDPR, are informed in accordance with GDPR and local requirements and, where necessary, are appropriately trained.

5.3. Roles and Responsibilities

Within its area of responsibility, the DMKS Management shall clearly define, regularly check, and document roles and responsibilities relating to the handling of Personal Data.

5.4. Data Protection Officer

Based on mandatory law DMKS has appointed a Data Protection Officer at the location of its Head Office. The Data Protection officer can be reached through the following means:

< Email: darshna_chp@yahoo.com,

The Data Protection Officer monitors compliance with the GDPR and other legal requirements, including the requirements of this Policy and Data Protection guidelines. The Data Protection Officer advises and informs the Executive Board and the Foundation's management regarding existing Data Protection obligations and is responsible for communicating with supervisory authorities. The Data Protection Officer checks selected processes at appropriate intervals on a random, risk-oriented basis to ensure their conformity with Data Protection guidelines. The Data Protection Officer performs their duties free from instructions and based on their expertise.

6. General Principles and Procedures

6.1. Information Security Framework: Availability, Confidentiality, and Integrity of Data

6.1.1. General Information Security Framework

To ensure the availability, confidentiality, and integrity of information, a general security framework shall be prepared based on the Information Security Policy, along with a risk analysis identifying protection needs, and shall set forth binding procedures for Processing information, including

Personal Data. The development of this framework should consider technical state of the art. The security framework shall be regularly reviewed and evaluated regarding the effectiveness of the organisational measures provided for therein. A classification system shall be established for the handling of information. All Employees shall be appropriately sensitised, including trainings, regarding the careful handling of information confidential and sensitive information, including Personal Data. The Information Security Policy regulates these issues in detail.

6.1.2. Risk Assessment on the Processing of Personal Data

Each Department or Project responsible for Processing Personal Data shall determine the protection required by of the kind of Processing activities as well as by the kind of Processed Personal Data; for that purpose the Department or Project shall take into consideration the nature, scope, circumstances, purposes of the Processing Personal Data as well as the probability of a potential Data Breach.

6.1.3. Obligation of Data Confidentiality

Employees are prohibited from collecting, Processing, or utilising Personal Data without authorisation. They must certify their agreement to treat Personal Data confidentially before taking up their employment duties, using the form provided for this purpose. Employees with special secrecy obligations must also agree to any such additional obligation in writing.

6.2. Schedule of Processing Activities

6.2.1. Obligation to Maintain a Register

The Head Office of DMKS shall maintain its records of Processing activities of Personal Data. Each Project shall name an individual who will document and maintain information on the required procedures of the respective Project, according to legal requirements and to this Policy. The Data Protection Officer may be consulted for advice.

6.2.2. Consolidated Register

The respective records of Processing activities of the Country Offices and the Head Office shall be consolidated in an appropriate manner, which shall be checked at regular intervals for accuracy, completeness, and consistency.

6.2.3. Submission

Upon request, DMKS will make the register available to the supervisory authority. The Data Protection Officer is responsible for doing this.

6.3. Data Protection Impact Assessment

If a Department or Project processes under its own responsibility Personal Data and such Processing is expected to create a high risk to the rights or freedoms of Data Subjects, it shall carry out Data Protection impact assessments before engaging in respective Processing. This particularly applies to the Processing of Personal Data of vulnerable Project Participants. A high risk exists, for example, if a large amount of Personal Data is being processed by default, if extensive Processing of Special Categories of Personal Data is to be carried out, if a comprehensive and systematic evaluation of personal characteristics of Data Subjects is to occur, or if the Processing operations are likely to present a high risk to a Data Subject in any other way. A Data Protection impact assessment is also required before the introduction of new data processing technologies. The Data Protection impact assessment must be documented in writing and include, at a minimum, the following content:

1. A systematic description of the envisaged Processing activity and the purpose of such Processing, including, where appropriate, any legitimate interests pursued by the Controller.
2. An assessment of the necessity and proportionality of the Processing activity in relation to the purpose;
3. An assessment of the risks to the rights and freedoms of Data Subjects and the safeguards to be taken to address those risks, including safeguards, security measures, and procedures to ensure the protection of Personal Data.

The Data Protection Officer shall advise the Department or Project carrying out the Data Protection impact assessment if the Processing activity may present a high risk to Data Subjects.

7. General Handling of Personal Data

7.1. Processing Only with Legal Authorisation

The Processing of Personal Data is generally prohibited, unless permitted by law. In principle, the GDPR allows for the Processing of Personal Data if and to the extent that:

1. The Processing is necessary for the performance of an existing contractual relationship with the Data Subject.

Example: The storage of necessary Personal Data within the framework of a consultancy contract or an employment relationship.

2. The Data Subject requested the Processing during pre-contractual communications, as well as while Processing a contract with the Data Subject.

Example: An interested donor requests informational material or verification about the general use of donations and then decides to donate. The data required to send the information and to process the donation (e.g., for issuing and sending the donation receipt) may be processed

3. The Data Subject has given their Consent.

Example: The Data Subject voluntarily registers to receive a newsletter or a Project Participants agrees to the Processing of Personal Data.

7.2. Principle of Data Minimisation

The Processing of Personal Data shall be aimed at Processing as little data as possible from Data Subjects. Personal Data may only be Processed to the extent necessary to achieve the legitimate purpose of the Processing. Personal Data must be anonymised or pseudonymised as far as this is possible, based on the purpose of use. For example, it will usually not be necessary to know and use the name of a Data Subject in the context of a statistical evaluation of data. Rather, this information can be replaced by a random value that also ensures that the underlying information is distinguishable.

7.3. Defining a Clear Processing Purpose

Personal Data may only be Processed for a specified, explicit, and legitimate purpose. Data Processing without a legitimate purpose, such as the storage of data by default, is not allowed.

7.4. Changing the Processing Purpose

Processing of Personal Data for a purpose other than that for which the Data Subject provided previous Consent is only allowed if the purpose of the further Processing is compatible with the purpose covered by the original Consent. the nature of the data processed, the consequences for the Data Subject, and the possibilities of encryption or Pseudonymisation must be considered. The Data Subject is to be comprehensively informed about such change of Processing purpose. The Data Protection Officer shall advise on the appropriate scope of the duty to inform.

7.5. Adequately Informing Data Subjects

When Personal Data is collected, the Data Subject shall be adequately informed about the handling of their data. This must include the purpose of the Processing, the identity of the Controller, the Recipients of the Personal Data, and all other information necessary to ensure fair and transparent Processing. The information shall be provided in an intelligible and easily accessible form and in as simple language as possible.

7.6. Data Collection from Third Parties / Subsequent Change of the Processing Purpose

If Personal Data is not collected from the data subject, but is procured, for example, from another company, the Data Subject must be subsequently and comprehensively informed about how their data is handled. The Data Protection Officer shall advise on the appropriate scope of the duty to inform.

7.7. Data Integrity

As far as this is possible with reasonable effort, DMKS shall ensure that Processed Personal Data is factually correct and, if necessary, up to date. The extent of data Processing must be necessary and relevant in relation to the defined Processing purpose. The responsible Department or Project shall ensure data integrity by establishing appropriate processes and regularly reviewing relevant databases in an appropriate manner to ensure that they are correct, necessary, and up to date.

8. Data Transfers

8.1. Special Permission

The transmission of Personal Data to Third Parties is only allowed based on law or on the Consent from the Data Subject.

8.2. Transfer to Countries outside of the European Union / EEA / International Organisations

Where the Recipient of Personal Data is located outside the European Union or the European Economic Area, or where the Recipient is an International Organisation, additional measures are necessary to safeguard the rights and interests of Data Subjects. A data transfer should not occur if an adequate level of Data Protection is not available at the receiving body or cannot be established – for example, by means of a special contractual clause.

9. Rights of Data Subjects

9.1. Right to Information

Data Subjects have the right to obtain information about any Personal Data processed by or on behalf of Welthungerhilfe. When Processing a request for information, the identity of the requestor must be established beyond doubt. If there are justified doubts as to their identity, additional information may be requested from the requestor. If the requestor's identity cannot be established beyond doubt, the information must be refused with a reason for the refusal provided in writing; if a Data Subject has submitted the request for information electronically, this may also be done electronically (e.g., via email).

9.2. Providing Information

Information is always provided in writing. If the Data Subject has submitted the request for information electronically, the information may also be provided electronically. The information shall include the Personal Data available as well as the Recipients of the Personal Data, the purpose of the Processing, and all other information required by law, so that the Data Subject can personally assess the lawfulness of the Processing. The Data Protection Officer shall advise on the necessary scope of the duty to provide information. At the specific request of the Data Subject, the data shall be made available in a structured, common, and machine-readable format. The responsible IT Department shall determine the standard to be provided for this purpose. Upon explicit request by the Data Subject a copy of the Personal Data shall be provided.

9.3. Correction

Data Subjects have the right to have their inaccurate Personal Data corrected. They may also request the completion of incomplete Personal Data. Requests for correction shall be complied with immediately.

9.4. Erasure the Data Subject has the right to erasure of their Personal Data under the following conditions:

1. Retention of the Personal Data is no longer necessary to fulfil the purposes of retention.
2. The Data Subject has withdrawn their Consent and there is no other legal basis for the Processing.
3. The Data Subject objects to Processing for direct marketing purposes or invoked a right of objection based on a specific – and justifiable – situation.
4. Special Categories of Personal Data are being Processed and their accuracy cannot be proven; or
5. There is another legal obligation to delete the Personal Data. If there is an obligation to delete Personal Data that has been previously made public, to the extent reasonably possible other data Processing Controllers must be informed of the request for deletion by the Data Subject with regard to all copies of and links to the respective Personal Data.

9.5. Restriction

The Data Subject may request a Processing Restriction on their Personal Data in the following circumstances:

1. The accuracy of the Personal Data is in dispute, but only for the period during which the accuracy is being verified by the responsible Department or Project; or
2. The Processing is unlawful, but the Data Subject refuses to have its Personal Data deleted; or
3. DMKS no longer needs the Personal Data for Processing purposes, but the Data Subject requires the Personal Data for the establishment, exercise, or defence of legal claims; or
4. The Data Subject has objected to the Processing based on a particular situation, and the responsible Project is still examining such objection.

9.6. Response Time

The Data Subject shall be informed within one month from the receipt of the request of the substantive measures taken in response to their request.

9.7. Right to Complain

Every Data Subject has the right to file a complaint about the Processing of their Personal Data if they feel their rights have been violated. Complaints may be submitted to the Data Protection Officer; the Data Protection Officer is independent and autonomous. Complaints may also be submitted to a supervisory authority.

9.8. Advisory Mandate of the Data Protection Officer

The Data Protection Officer shall be available to advise on protecting the rights of Data Subjects.

10. Training

Employees who have ongoing or regular access to Personal Data, who process such data (e.g., Employees of the Human Resources Department, the Donor Unit, or Project staff who process Project Participants data), or who develop or maintain systems for Processing such data shall be trained in an appropriate manner on Data Protection obligations.

11. Audits

11.1. Regular Review of the Level of Data Protection

To ensure an appropriate level of Data Protection, relevant processes shall be regularly reviewed under the responsibility of the Internal Audit Department by internal or external bodies. If a possibility for improvement is identified, corresponding corrective measures shall be identified and implemented in accordance with an action plan.

11.2. Duties with Respect to Documentation and Information

Audit findings shall be documented. This documentation shall be handed over to the Data Protection Officer. Those responsible for the processes audited shall be informed of the results.

11.3. Completion of the Audit

An audit is successfully completed when all improvement measures recommended in the report have been appropriately implemented. The respective Department or Project, within whose scope the processes to be improved fall are responsible for the implementation of the improvement measures. They report on the progress and completion of the improvement measures to the DMKS Management. As needed, follow-up audits may be carried out to verify the effective implementation of the recommended improvement measures.

12. Internal Investigations

12.1. Compliance with Data Protection Law

Investigation measures to clarify the facts of a case or to prevent or detect criminal offences or serious breaches of duty in the employment relationship shall be carried out in strict compliance with relevant Data Protection laws and regulations. Any associated collection and use of Personal Data to achieve the purposes of the investigation must be necessary, appropriate, and proportionate to the interests of the Data Subject.

12.2. Duty to Inform the Data Subject

The Data Subject shall be informed as soon as possible and as appropriate of the investigation measures taken with respect to them.

12.3. Involvement of the Data Protection Officer and Employee Representative

In all internal investigation proceedings, the Data Protection Officer must be consulted in advance on the selection and design of the measures envisaged to verify their conformity with applicable Data Protection law. Likewise, the relevant employee representative body must be appropriately informed or involved in line with applicable law.

13. Accountability

Compliance with the requirements of this Policy must always be ascertainable. Particular attention must be paid here to the auditability and transparency of measures taken, for example, by means of associated documentation.

14. Updating the Policy

This Policy shall be regularly reviewed with an eye towards adapting and amending it in the context of further development of Data Protection law, as well as technological and organisational changes. Any change to this Policy must be approved by the board members and data protection Officer and must be documented promptly in writing. Employees must be informed of changes to the Policy in a prompt and appropriate manner.

15. Complaints, Duty to Report, and Consequences of Violations

15.1. Duty to Report

Employees who know or suspect violations of this Policy are obliged to report them immediately to their manager or, if deemed more appropriate, to the Privacy Officer or the Compliance Department at the DMKS Head Office. Any suspicion of a material violation of this Policy provided to a manager directly or via a DMKS complaints mechanism must be reported immediately by the manager to the Compliance Department. Reports can be made to the Compliance Department via a confidential email address. In addition, DMKS allows anonymous reporting on the Internet or by telephone via a whistleblowing hotline:

Internet: www.ngodarshna.org

Whistleblowing hotline: +91-7747007502

All information about violations of this policy will be handled in a strictly confidential manner. No one who in good faith reports any violation, suspicion of a violation, or evidence of a violation need fear disadvantages or other negative consequences as a result of making this report, even if the report, suspicion, or evidence later turns out to be unfounded. It is not the duty or responsibility of the reporting person to independently investigate or decide whether a Data Protection violation has occurred. The following documents provide more detailed information:

This Policy was approved by the Board Members of Darshna Mahila Kalyan Samiti, Chhatarpur on […] 2020.

Rajesh Gupta
Treasurer of DMKS

Prabha Vaidya
Secretary of DMKS