# RENEW MICROFINANCE PRIVATE LIMITED


**INTERNAL DATA PRIVACY AND PROTECTION POLICY 2022**

RENEW Microfinance Private Limited (RENEW MFPL) is committed to compliance with data protection laws and regulations. Protecting the confidentiality and integrity of personal data is a critical responsibility. The Internal Data Privacy and Protection Policy is intended to ensure that we comply with Guidelines on Data Privacy and Data Protection and follow good practice and protect the rights of the employees and the clients. RENEW MFPL aims to ensure that individuals are aware that their data is being processed, and that they understand how the data is being used and how to exercise their rights.

## TABLE OF CONTENT


| SI No | Content | Page No. |
|---|---|---|
| 1 | Scope of the data protection policy | 3 |
| 2 | Definition | 3 |
| 3 | Principles for processing personal data | 4-5 |
| 4 | Data Processing | 5-6 |
| 5 | Confidentiality | 6 |
| 6 | Processing security | 7 |
| 7 | Record keeping | 7 |
| 8 | Responsibilities of the employees | 8-9 |
| 9 | Violation, sanction, and reporting | 9 |

## 1. SCOPE OF THE DATA PROTECTION POLICY

Data Protection Policy applies to all personal data that RENEW MFPL process relating to identifiable individuals. This Data Protection Policy applies to all RENEW MFPL staff and stakeholders.

## 2. DEFINITION

### 2.1 Data Privacy

Data Privacy is defined as the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information.

### 2.2 Data Protection

Data Protection is defined as the implementation of appropriate administrative, technical, or physical means to guard against unauthorized intentional or accidental disclosure, modification or destruction of data.

### 2.3 Personal Data or Personal Information

Personal data herein referred to, means any data or information relating to a natural person who is or can be identified from that data.

This can include in particular:

- Names of individual
- Address
- Email address
- Telephone/Mobile number
- Citizenship Identity Card
- Date and place of birth.

### 2.4 Personal Data Processing

Processing of personal data means any operation or set of operations that is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, retention, modification, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, deletion, or destruction.

## 3. PRINCIPLES FOR PROCESSING PERSONAL DATA

### 3.1 Fair and lawful

a. When processing personal data, the individual rights of the data subjects must be protected.
b. Personal data must be collected and processed in a fair and lawful manner.
c. Collected data shall be adequate, relevant, and not excessive in relation to the purposes for which they are obtained and their further processing.
d. Individual data can be processed upon consent of the data subject.
e. Personal data shall be obtained only for specified, explicit and legitimate purposes.

### 3.2 Transparency

The data subject must be informed of how his/her data is being handled. When the data is collected, the data subject must either be made aware of:

a. Information about the purpose of processing
b. Contact detail of Data Protection Officer
c. Information about lawful basis of processing
d. Information on how the personal data was obtained, if not directly from the data subject
e. Information on how the data subject can withdraw consent
f. Information about transfers of personal data
g. Information about recipients or categories of recipients of personal data
h. Information about the period for which the personal data is retained.

### 3.3 Confidentiality and Data Security

a. Personal data must be treated as confidential and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing, or distribution, as well as accidental loss, modification, or destruction.
b. All employees of RENEW MFPL with access to personal data are subject to confidentiality obligation.
c. All access to personal data shall be logged. Data access logs shall record access to personal data including who accessed, when and which individual's personal data was accessed and what changes, if any, were done to the data.

### 3.4 Deletion

a. Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed.
b. Document any use of removable media and/or devices for the storage of personal data.
c. Ensure that the use of mobile devices does not lead to compromise of personal data.
d. Shall have documented backup policy which addresses the requirement for backup, recovery, and restoration of personal data.

### 3.5 Accuracy

a. Personal data on file must be correct, complete, and kept up to date.
b. The staff must check the accuracy of any data at the point of collection and at regular intervals.
c. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, or updated.

## 4. DATA PROCESSING

### 4.1 Consent to Data Processing

Individual data can be processed upon consent of the person concerned. Declarations of consent must be submitted voluntarily.

### 4.2 Rights of the Data Subject

All individuals who are the subject of personal data held by RENEW MFPL are entitled:

a. To request information on which personal data relating to him/her has been stored, how the data was collected, and for what intended purpose.
b. If personal data is transmitted to third parties, individuals should be informed of such a possibility.
c. If personal data is incorrect or incomplete, the data subject can demand that it be corrected or supplemented.
d. To request his/her data to be deleted if the processing of such data has no legal basis, or if the legal basis has ceased to apply. The same applies if the purpose behind the data processing has lapsed or ceased to be applicable for other reasons. Existing retention periods and conflicting interests meriting protection must be observed.

### 4.3 Transmission of Personal Data

a. Transmission of personal data to recipients outside or inside RENEW MFPL is subject to the authorization requirements for processing personal data and requires the consent of the data subject.
b. The data recipient must be required to use the data only for the defined purposes.
c. If data is transmitted to a recipient outside RENEW MFPL, this recipient must agree to maintain a data protection. This does not apply if transmission is based on a legal obligation.
d. The processing of personal data is permitted if national legislation requests, requires or authorizes this. In certain circumstances, the RENEW MFPL Data Protection Policy allows personal data to be disclosed, based on a legal obligation, to law enforcement agencies, without the consent of the data subject.
e. Only the CEO and the Data Protection Officer can validate any such disclosure in writing, ahead of the disclosure, after ensuring the request is legitimate, motivated by the requester, appropriate, necessary and does not pose a threat or direct risk to RENEW MFPL.

## 5. CONFIDENTIALITY

a. Personal data is subject to data secrecy.
b. Any unauthorized collection, processing, or use of such data by employees is prohibited.
c. Any data processing undertaken by an employee that he/she has not been authorized to carry out as part of his/her legitimate duties is unauthorized.
d. Duly authorized employees may have access to personal information only as is appropriate for the type and scope of the task in question.
e. Employees are forbidden to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way.
f. Employees must sign the confidentiality obligation to protect data secrecy. This obligation shall remain in force even after employment has ended.

## 6. PROCESSING SECURITY

a. Personal data must be safeguarded from unauthorized access and unlawful processing or disclosure, as well as accidental loss, modification, or destruction. This applies regardless of whether data is processed electronically or in paper form.
b. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented.

## 7. RECORD KEEPING

RENEW MFPL will keep full and accurate records of data processing activities, such as:

a. Data subjects' consent for processing their data
b. The type of processing
c. The purpose of data processing
d. Description of categories of personal data and the data subjects.
e. The categories of recipients to whom the personal data will be disclosed or has been disclosed.
f. Keep a record of which personal data have been communicated, when and to whom.
g. A general description of the technical and security measures.
h. A privacy impact assessment report.

## 8. RESPONSIBILITIES OF THE EMPLOYEES

The Employee shall be diligent and extend caution while dealing with Personal Data of the clients, during performance of his/her duties.

a. Abide by RENEW MFPL Internal Data Privacy Policy.
b. Hold the personal data in strict confidence and protect the confidentiality, integrity, and availability of such data/information.
c. Prevent any unauthorized person from having access to any computer systems processing personal data.
d. Ensure that authorized users can access only the personal data to which their access right refers.
e. Keep a record of which personal data have been communicated, when and to whom.

f. Not disclose or divulge either directly or indirectly, the personal data to others unless authorized to do so in writing by the Chief Executive Officer or the Data Protection Officer.
g. Ensure that, during communication of personal data and transfer of storage media, the data cannot be read, copied, or erased without authorization.
h. Immediately, on becoming aware report and notify any vulnerabilities and privacy related breach/security breaches.
i. Attend trainings on security and data privacy.

## 9. VIOLATION, SANCTION, AND REPORTING

a. Any failure to comply with the policy or to deliberately violate the clauses set in the policy will result in immediate disciplinary action or dismissal.
b. Depending on the nature, circumstances and location of the case and violation, RENEW MFPL will also consider involving authorities such as the police to ensure the protection of personal data and victims.
c. The reporting of suspected or actual violations to this policy is a professional and legal obligation of all staff. Failure to report information may lead to initiation of appropriate disciplinary actions including but not limited to employee dismissal/termination.
d. Every employee who deals with personal data, shall have a responsibility to comply with the applicable law concerning data privacy and the Guidelines on Data Privacy and Protection 2022.