DATA PRIVACY POLICY

(Information & Cybersecurity Procedure Ver 1.2 – Data Privacy)

Document details	
Document reference	Asirvad/ISMS/Procedure/A01
Next Review Date	January 2023
Owned by	**IT Strategy Committee**
Implemented by	CISO
Governed by	**IT Strategy Committee**

Revision history

Version No.	Date	Details of Change	Changes done by	Changes	Approved By/Date
1.0	August 2020	Initial Version	Sundararajan S	DATA PRIVACY POLICY	**Board Approved**
1.0	Jan 2022	Review	CISO	No Change Required	

Policy Statement

The purpose of this policy is to maintain the privacy of and protect the personal information of customers, employees, contractors, vendors, and business partners of Asirvad Microfinance Limited and ensure compliance with laws and regulations applicable to Asirvad Microfinance Limited (hereafter referred to as "AML" or "the organization"). This policy must be read in conjunction with the online privacy policy published on Asirvad website.

Scope

This policy is applicable to all AML employees, contractors, vendors, customers, and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization.

This Policy applies to all AML employees, contractors, vendors, customers, and business partners who receive personal information from AML, who have access to personal information collected or processed by AML, or who provide information to AML, regardless of geographic location.

All employees of AML are expected to support the privacy policy and principles when they collect and/or handle personal information or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization's commitment towards data privacy.

All subsidiaries and any Third-Party working with or for AML, and who have or may have access to personal information, will be expected to have read, understand, and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

As per AML business process, personally identifiable information (PII) is collected/stored in the following areas

- www.Asirvadmicrofinance.co.in
- Asirvad branch application,
- customer onboarding module,
- mobile app for customer onboarding,
- LOS/LMS module (structured loans)
- ESS web module (lead management)
- Asirvad OGL web application
- Asirvad OGL mobile applications (OGL and OGL lite)
- Asirvad Glow/ Trucell/ Br.Net/ Analytics mobile application
- HRMS (employee details)
- Procurement (vendor details)
- NCD (depositor details)
- CRM/call center module, Dialer module
- Asirvad ESS mobile application (lead management)
- Asirvad board meeting web and mobile/tablet application
- Asirvad Br.Net Application

Responsibilities

The owner for the Data Privacy Policy shall be the ISMS Officer. The ISMS Officer shall be responsible for maintenance and accuracy of this policy.

This policy shall be reviewed for updates by IT Strategy committee on an annual basis. Additionally, the data privacy policy shall be updated in-line with any major changes within the organization's operating environment, on recommendations provided by internal/ external auditors and/or on any changes brought in by regulatory/statutory amendments.

Policy Compliance

Compliance to the data privacy policy shall be reviewed on an annual basis by compliance department to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes.

In cases where non-compliance is identified, the ISMS officer shall review the reasons for such non-compliance along with a plan for remediation and report them to compliance department. Depending on the conclusions of the review, need for a revision to the policy may be identified. In instances of persistent non-compliance by the individuals concerned, they shall be subject to action in accordance with the AML disciplinary process.

Data Privacy Principles

This Policy describes reasonable security practices (RSP) and Generally accepted privacy principles (GAPP) for the protection and appropriate use of personal information at AML. These principles shall govern the use, collection, disposal, and transfer of personal information, except as specifically provided by this Policy or as required by applicable laws:

Notice: AML shall provide data subjects with notice about how it collects, uses, retains, and discloses personal information about them.
Choice and Consent: AML shall give data subjects the choices and obtain their consent regarding how it collects, uses, and discloses their personal information.
Rights of Data subject: AML shall provide individuals with the right to control their personal information, which includes the right to access, modify, erase, restrict, transmit, or object to certain uses of their information and for withdrawal of earlier given consent to the notice.
Collection: AML shall collect personal information from data subjects only for the purposes identified in the privacy notice / SoW / contract agreements and only to provide requested product or service.
Use, Retention and Disposal: AML shall only use personal information that has been collected for the purposes identified in the privacy notice / SoW / contract agreements and in accordance with the consent that the data subject shall provide. AML shall not retain personal information longer than is necessary to fulfil the purposes for which it was collected and to maintain reasonable business records. AML shall dispose the personal information once it has served its intended purpose or as specified by the data subject.
Access: AML shall allow data subjects to make inquiries regarding the personal information about them, that AML shall hold and, when appropriate, shall provide access to their personal information for review, and/or update.

Disclosure to Third Parties: AML shall disclose personal information to Third Parties / subsidiaries only for purposes identified in the privacy notice / SoW / contract agreements. AML may also disclose such personal information as and when required by the laws of the land may be in force from time to time. AML shall disclose personal information in a secure manner, with assurances of protection by those parties, according to the contracts, laws, and other segments, and, where needed, with consent of the data subject.

Obligations for Sub-processor: Where a processor (vendor or third party acting on behalf of AML 's data processor) engages another processor (Sub-processor) for carrying out specific processing activities on behalf of AML (controller), the same data protection obligations as set out in the contract or other legal act between AML and the processor shall be imposed on the Sub-processor by way of a contract or other legal Act, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Information Technology Act, India and its amendments. Where the Sub-processor fails to fulfil its data protection obligations, the initial processor (relevant vendor or third party acting on behalf of AML's data processor) shall remain fully liable to AML for the performance of that Sub-processor's obligations.

Security for Privacy: AML shall reasonably protect personal information from unauthorized access, data leakage and misuse.

Quality: AML shall take steps to ensure that personal information in its records is accurate and relevant to the purposes for which it was collected.

Monitoring and Enforcement: AML shall monitor compliance with its privacy policies, both internally and with Third Parties, and establish the processes to address inquiries, complaints, and disputes.

Notice

Notice shall be made readily accessible and available to data subjects before or at the time of collection of personal information or otherwise, notice shall be provided as soon as practical thereafter. Notice shall be displayed clearly and conspicuously and shall be provided through online (e.g. by posting it on the website/intranet portal/mobile applications) and/or offline methods (e.g. through posts, couriers, etc.). All the web sites (including Intranet portals), and any product or service that collects personal information internally, shall have a privacy notice. In case of any cross-border transfer of personal information, the data subjects shall be informed by a notice sufficiently prior to the transfer.

Privacy notices may include:

- the organization's operating jurisdictions: Third Parties involved; business segments and affiliates; lines of business; locations.
- types of personal information collected; sources of information; who is collecting the personal information, including contact information.
- the purpose of collecting the personal information.
- assurance that the personal information will be used only for the purpose identified in the notice and only if the implicit and/or explicit consent is provided unless a law or regulation specifically requires otherwise.
- any choices the data subject have regarding the use or disclosure of the information; the process and data subject shall follow to exercise the choices.
- the process for a data subject to change contact preferences and ways in which the consent is obtained.

- collection process and how the information is collected; how the information is used including any onward transfer to Third Parties.
- retention and disposal process for personal information; assurance that the personal information to be retained only as long as necessary to fulfill the stated purposes, or for a period specifically required by law or regulation and will be disposed-off securely or made anonymous post the identified purpose is completed.
- process of accessing personal information; the costs associated for accessing personal information (if any); process to update / correct the personal information; the resolution of disagreements related to personal information.
- how the information is protected from unauthorized access or use.
- how users will be notified of any changes made to privacy notice.
- disclosure process for Third Parties; the assurance that the personal information is disclosed to Third Parties only for the purpose identified; the remedial actions in place for any misuse of personal information by the Third Parties.
- security measures in place to protect the personal information; ways of maintaining quality of personal information.
- monitoring and enforcement mechanisms in place; description of the complaint channels available to data subjects; how the internal personnel, key stakeholders and the customers can contact the organization related to any privacy complaints or breaches; relevant contact information and/or other reporting methods through which the complaints and/or breaches could be registered.
- Consequences of not providing the requested information.

Choice and consent

Choice refers to the options for the data subjects are offered regarding the collection and use of their personal information. Consent refers to their agreement to the collection and use, often expressed by the way in which they exercise a choice option.

- AML shall establish systems for the collection and documentation of data subject consents to the collection, processing, and/or transfer of personal data.
- Data subjects shall be informed about the choices available to them with respect to the collection, use, and disclosure of personal information.
- Consent shall be obtained (in writing or electronically) from the data subjects before or at the time of collecting personal information or as soon as practical thereafter.
- The changes to a data subject's preferences shall be managed and documented. Consent or withdrawal of consent shall be documented appropriately.
- The choices shall be implemented in a timely fashion and respected. If personal information is to be used for purposes not identified in the notice / SoW / contract agreements at the time of collection, the new purpose shall be documented, the data subject shall be notified, and consent shall be obtained prior to such new use or purpose.
- The data subject shall be notified if the data collected is used for marketing purposes, advertisements, etc.
- AML shall review the privacy policies of the Third Parties and types of consent of Third Parties before accepting personal information from Third Party data sources.

Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information.

- Personal information shall not be collected unless either of the following is fulfilled:
  - the data subject has provided a valid, informed, and free consent.
  - processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering a contract.
  - processing is necessary for compliance with the organization's legal obligation.
  - processing is necessary in order to protect the vital interests of the data subject.
  - processing is necessary for the performance of a task carried out in the public interest
- Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labelled as optional. Collection of personal information shall be avoided or limited when reasonably possible.
- Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost.
- When using vendors to collect personal information on the behalf of AML, it shall ensure that the vendors comply with the privacy requirements of AML as defined in this policy.
- AML shall at minimum, annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose.
- Respective department/function shall obtain approval from the CTO before adopting the new methods for collecting personal information electronically.
- AML shall review the privacy policies and collection methods of Third Parties before accepting personal information from Third-Party data sources.

Use, Retention and Disposal

- Personal information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the data subject has given consent.
- Personal information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the data subjects.
- When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable.
- AML shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects who are authorized to request those changes.
- Personal information shall be erased if the storage violates any of the data protection rules or if knowledge of the data is no longer required by AML or for the benefit of the data subject. Additionally, AML has the right to retain the personnel information for legal and regulatory purpose and as per applicable data privacy laws.

- AML shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed-off in compliance with the organization's data privacy policy.

Access

AML shall establish a mechanism to enable and facilitate exercise of data subject's rights of access, blockage, erasure, opposition, rectification, and, where appropriate or required by applicable law, a system for giving notice of inappropriate exposure of personal information.

- Data subjects shall be entitled to obtain the details about their own personal information upon a request made and set forth in writing. AML shall provide its response to a request within 72 hours of receipt of written request.
- The data subjects shall have the right to require AML to correct or supplement erroneous, misleading, outdated, or incomplete personal information.
- Requests for access to or rectification of personal information shall be directed, at the data subject's option, to the respective head of department of the projects team or support function responsible for the personal information.
- The privacy coordinators shall record and document each access request as it is received, and the corresponding action taken.
- AML shall provide personal information to the data subjects in a plain simple format which is understandable.

Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal information shall be disclosed to Third Parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

- Personal information of data subjects may be disclosed to the Third Parties / subsidiaries only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law.
- AML shall notify the data subjects prior to disclosing personal information to Third Parties/ partner firms for purposes not previously identified in the notice / SoW / contract agreements.
- AML shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the Third Parties / subsidiaries.
- The Third Parties shall sign an NDA (Non-Disclosure Agreement) with AML before any personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of Personally identifiable information (PII).

Security

Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred, and disposed by AML

- Information asset labelling and handling guidelines shall include controls specific to the storage, retention, and transfer of personal information.
- AML shall establish procedures that maintain the logical and physical security of personal information.

- AML shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards.
- Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.

Quality

AML shall maintain data integrity and quality, as appropriate for the intended purpose of personal data collection and use and ensure data is reliable, accurate, complete, and current.

- For this purpose, the nodal/data protection officer shall have systems and procedures in place to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.
- AML internal audit department shall perform an annual assessment on the personal information collected to check for accuracy, completeness, and relevance of the personal information.

Monitoring and enforcement

Dispute Resolution and Recourse: AML shall define and document an Incident management policy (refer AML INCIDENT MANAGEMENT) which addresses the privacy related incidents and breaches.

- The incident and breach management program include a clear escalation path up to the executive management, legal department, and the board based on type and/or severity of the privacy incident/breach. It shall define a process to register all the incidents/complaints and queries related to data privacy.
- AML Grievance Officer shall perform a periodic review of all the complaints related to data privacy to ensure that all the complaints are resolved in a timely manner and resolutions are documented and communicated to the data subjects.
- An escalation process for unresolved complaints and disputes which shall be designed and documented.
- Communication of privacy incident / breach reporting channels and the escalation matrix shall be provided to all the data subjects.

Dispute Resolution and Escalation Process for Employees: Employees with inquiries or complaints about the processing of their personal information shall first discuss the matter with their immediate supervisor. If the employee does not wish to raise an inquiry or complaint with an immediate manager, or if the manager and employee are unable to reach a satisfactory resolution of the issues raised, the employee shall bring the issue to the attention of the Grievance Officer whose details are as mentioned below.

Name	Mrs. **Radhika**
Contact Number	**9361912512**
E-mail	grievance@asirvad.in
Working Days / Hours	Monday to Friday / 9:30 am to 6:30 pm

Dispute Resolution and Escalation Process for Customer / Third Party

Customers / Third Party with inquiries or complaints about the processing of their personal information shall bring the matter to the attention of the Grievance Officer in writing. Any disputes concerning the processing of the personal information of non-employees shall be resolved through arbitration.

Compliance Review

Internal audit team shall conduct an internal audit annually (at minimum) to ensure compliance with the established privacy policies and applicable laws.

- The internal audit shall consist of the review of the following:
  - personal information collected from data subjects.
  - the purposes of the data collection and processing.
  - the actual uses of the data.
  - disclosures made about the purposes of the collection and use of such data.
  - the existence and scope of any data subject consents to such activities.
  - any legal obligations regarding the collection and processing of such data, and
  - the scope, sufficiency, and implementation status of security measures.
- The internal audit team shall document all the instances of non-compliance with privacy policies and procedures and report the same with the Privacy Management committee.
- The Nodal/Data Protection Officer shall take actions on the findings from the internal audit and work on the recommendations for improvement of the privacy posture.
- Any changes made to the policies shall be communicated to all the employees, the stakeholders, and the customers / clients.

Glossary

Term	Definition
Data Subject	A data subject who is the subject of personal and sensitive personal data.
Personal data or Personally Identifiable Information (PII)	PII is any information about an individual (the data subject) which can • any information that can be used to distinguish or trace an individual's identity, • any other information that is linked or linkable to an individual Examples included but not limited to: Name, Address, Date of birth etc.
Sensitive Personal Information (SPI)	Sensitive personal data means personal data consisting of information but not limited to the following attributes of the data subject: • password • financial information such as bank account or credit card or debit card • or other payment instrument details, • physical, physiological, and mental health condition, • sexual orientation,

	• medical records and history, • genetic or biometric information, • racial and ethical origin, • political opinions, • religious or philosophical beliefs, • trade union membership, • any detail relating to the above clauses as provided to body corporate for providing service; and • any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 as amended from time to time or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.
Third Party	All external parties, including contractors/vendors, state and central government agencies and other statutory authorities – who have access to AML information assets or information systems.
Data protection and security	Anyone collecting personal and customer information must fairly and lawfully process it, process it only for limited, specifically stated purposes, use the information in a way that is adequate, relevant, and not excessive, use the information accurately, keep the information on file no longer than absolutely necessary, process the information in accordance with your legal rights, keep the information secure and never transfer the information outside the country without adequate protection.