



Document Title : Personal Data Privacy Policy

Document Control:	
Policy Name	Personal Data Privacy Policy
Policy Author/Owner	IT Department
Policy Reviewer	Head of IT
Policy Approver	Board
Document Classification	Internal
Document Contact Point	IT Team

Revision History:				
Version No.	Date	Proposed by	Approved by	Reason For New Release
1.0	12-Nov-2024	Head of IT	Board	1 st Released - UIDAI Norms
1.1	05-Nov-2025	Head of IT	Board	No revisions required (Annual Review)
1.2	29-Jan-2026	InfoSec Team	Board	Addition of Clause 15



1. Introduction

Midland Microfin, a trusted financial institution dedicated to serving its valued clientele, is committed to safeguarding the privacy and security of personal data. In adherence to the Digital Personal Data Protection Act of 2023, Midland Microfin proudly presents its updated and comprehensive Personal Data Privacy Policy. This policy serves as an unequivocal commitment to protecting the privacy rights of its users and supersedes all previous policies. With a steadfast focus on compliance and transparency, Midland Microfin aims to build and maintain trust while ensuring the highest standards of data protection for its customers.

1.1 Purpose of the Privacy Policy

The purpose of Midland Microfin's Privacy Policy is to outline the principles and guidelines that govern the collection, use, disclosure, and protection of personal data. This policy serves as a transparent and comprehensive document that informs individuals about how their personal information will be handled by Midland Microfin. It aims to establish a clear understanding of the organization's commitment to data privacy, ensuring that individuals are aware of their rights, the purposes for which their data is processed, and the measures in place to protect their information. By defining the purpose of this Privacy Policy, Midland Microfin seeks to promote trust, accountability, and compliance with the Digital Personal Data Protection Act of 2023, ultimately fostering a secure and respectful data privacy environment for its stakeholders.

1.2 Scope of the Privacy Policy

The scope of Midland Microfin's Privacy Policy is extensive and encompasses all aspects of the organization's data privacy practices. This policy applies to every individual whose personal data is collected, processed, or stored by Midland Microfin, whether they are customers, employees, partners, or other stakeholders. It covers all interactions, both online and offline, through which personal data is gathered, including the use of Midland Microfin's website, mobile applications, in-person meetings, and other communication channels.



In summary, the scope of this policy is broad, encompassing all aspects of data privacy within Midland Microfin and serving as the primary document governing the organization's data handling practices in accordance with the 2023 Act.

1.3 Definitions

In the context of Midland Microfin's Privacy Policy, several key terms and definitions are essential to ensure clarity and understanding. These definitions help stakeholders comprehend the specific terminology used throughout the policy:

1. **Personal Data:** Personal data refers to any information that relates to an identified or identifiable individual (Borrowers/Staff). This includes, but is not limited to, names, addresses, email addresses, phone numbers, financial data, and any other data that can be used to identify an individual.
2. **Sensitive Information:** Sensitive information includes a subset of personal data that requires special protection due to its potential for harm if disclosed or misused. This may encompass financial information, health records, government-issued identification numbers, and other data categories specified by applicable laws and regulations.
3. **Data Collection Methods:** Data collection methods describe the various ways in which Midland Microfin gathers personal data. These methods can include online forms, in-person interviews, mobile applications, website cookies, and other mechanisms.
4. **Data Processing:** Data processing encompasses all activities related to personal data, including collection, storage, use, sharing, and deletion. It covers both automated and manual processes.
5. **Marketing:** Marketing refers to the use of personal data for promotional or advertising purposes, such as sending newsletters, product recommendations, and targeted advertisements.
6. **Automated Decision-Making:** Automated decision-making involves the use of algorithms and technology to make decisions, often without human intervention. This can impact individuals' rights and choices, and Midland Microfin ensures transparency in such processes.
7. **Data Security:** Data security refers to the measures and safeguards implemented to protect personal data from unauthorized access, breaches, or cyber threats.
8. **Access Control:** Access control pertains to the policies and procedures in place to manage who has access to personal data within the organization and under what conditions.



9. **Data Encryption:** Data encryption involves the transformation of personal data into a coded format to prevent unauthorized access or interception during transmission or storage.
10. **Data Retention and Deletion:** Data retention and deletion policies dictate how long personal data is stored and when it should be permanently deleted in compliance with legal requirements.
11. **Third-Party Data Processors:** Third-party data processors are external entities that Midland Microfin may engage to handle personal data on its behalf, subject to strict data protection agreements.

These definitions serve as the foundation for understanding the key terms and concepts used throughout Midland Microfin's Privacy Policy, ensuring transparency and clarity in data privacy discussions and practices.

1. Information the organisation collects

1. Midland Microfin employs various methods to collect data in its pursuit of delivering financial services effectively and responsibly. These methods include online loan application forms, in-person interviews, mobile applications, and website cookies. By utilizing these techniques, Midland Microfin ensures the secure gathering of data from its clients. Data must be encrypted and kept in a database containing the Aadhaar number. Encryption keys need to be safely stored, ideally with HSMs. Simple spreadsheets must be safely saved and password-protected if they are to be used.

(Refer to Compendium of regulations, circulars and guidelines- Section-3- other circulars and guidelines- Do's for Aadhaar user Agencies/Departments.)

2.1 Types of Personal Data Collected

In terms of the types of personal data collected, Midland Microfin covers a wide spectrum. This includes identity information such as names, addresses, contact details, and government-issued identification numbers. Additionally, financial data, encompassing income details, credit history, bank account information, and other related financial information, is collected to assess eligibility and manage financial services effectively. The organization must assign a person to be in charge of safeguarding personal information connected to Aadhaar. That individual must to have responsibility in charge of auditing, access control, system security, etc. Identify and restrict any possible data leak or release of personal information. Make sure that any breach involving personal data is handled quickly.



(Refer to Compendium of regulations, circulars and guidelines- Section-3- other circulars and guidelines-Do's for Aadhaar user Agencies/Departments.)

2.2 Collection of Sensitive Information

Recognizing the importance of sensitive information, Midland Microfin exercises caution and collects such data only when necessary for specialized financial services, always with explicit consent from the individuals involved.

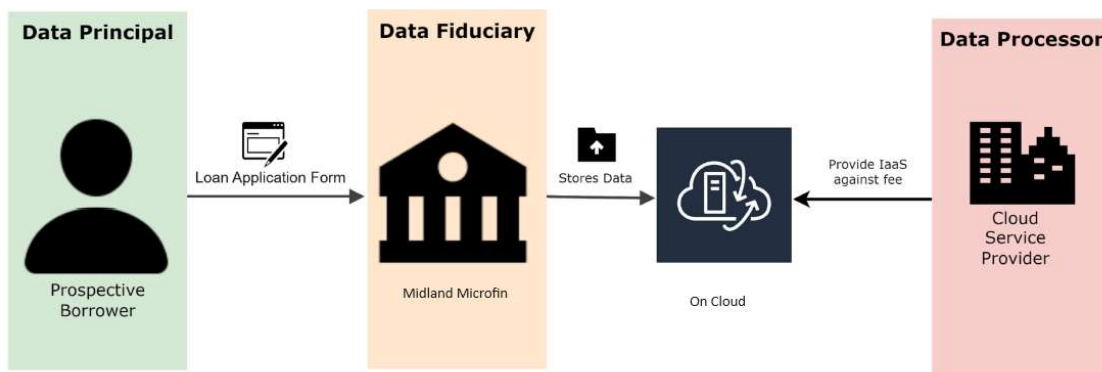
(Refer to Compendium of regulations, circulars and guidelines- AADHAAR (DATA SECURITY) REGULATION, 2016 – 5(h))

2.3 Collection from Minors

Regarding data collection from minors, Midland Microfin strictly adheres to legal regulations. The organization does not intentionally collect personal data from minors below the legal age without verified parental consent. If any data is inadvertently collected from minors, Midland Microfin promptly takes appropriate measures to delete it, ensuring compliance with data protection regulations and ethical standards.

2. How the organisation uses the individual's information

The company is dedicated to safeguarding the privacy and security of personal data belonging to individuals. This is however demonstrated through its commitment to data protection by outlining how it utilizes personal information while maintaining compliance with the DPDP Act.



3.1 Purpose of Data Processing



Midland processes personal data for specific and lawful reasons, as articulated in its privacy policy. These objectives may encompass:

- Delivering and enhancing the products or services offered by Midland.
- Executing contractual obligations with customers.
- Ensuring the safety and integrity of customer accounts.
- Adhering to legal and regulatory obligations.

3.2 Legal Basis for Data Processing

Midland relies on legally permissible grounds for processing personal data, as stipulated by the DPDP Act. These grounds include:

- **Consent:** Midland acquires explicit consent from its individuals before processing their personal data for well-defined purposes.
- **Contractual Necessity:** Data processing is carried out when necessary to fulfil agreements with customers or to provide requested services.
- **Legal Obligations:** Compliance with legal mandates and regulatory prerequisites.
- **Legitimate Interests:** Processing personal data when it serves legitimate interests, always ensuring that the rights and interests of individuals are not compromised.

3.3 Data Processing for Marketing

As part of its business operations, Midland may engage in marketing activities, necessitating the processing of personal data. These activities may encompass:

- Sending promotional messages or emails.
- Conducting market research.
- Tailoring advertisements based on individuals' preferences.

Midland guarantees that individuals have the option to decline marketing communications, in full adherence to the DPDP Act's requirements for consent and notification.

3.4 Automated Decision-Making

Midland may employ automated systems and algorithms for decision-making processes. These decisions can have implications for individuals in various contexts, such as credit assessments or product recommendations. However, Midland strictly follows the provisions of the DPDP Act, ensuring transparency in automated decision-making procedures and granting individuals the right to contest decisions made solely through automated means.



It's important to note that this example is entirely fictional, and the actual data processing practices of "Midland" would be contingent on its specific operations and its interpretation and compliance with the DPDP Act and other relevant laws and regulations.

3. Data Protection Measures

In accordance with the Digital Personal Data Protection Act, 2023 (DPDP Act), Midland shall prioritize comprehensive data protection measures to safeguard individuals' personal information. They must ensure compliance with all applicable laws and regulations related to data storage and protection of Aadhaar-based identity information across their systems, their agents' systems (if applicable), and authentication devices.

(Refer to Compendium of regulations, circulars and guidelines- Section1- Aadhaar regulations- Point no. 17(g))

4.1 Data Security:

Midland places a strong emphasis on data security to safeguard personal information. This entails implementing robust measures to protect data from unauthorized access, disclosure, alteration, and destruction. These security measures include:

- **Firewalls and Intrusion Detection Systems:** Midland employs advanced firewalls and intrusion detection systems to prevent unauthorized access to its data repositories.
- **Regular Security Audits:** Routine security audits and vulnerability assessments are conducted to identify and rectify potential weaknesses in the data security infrastructure.
- **Encryption:** Sensitive data is encrypted during transmission and storage to ensure that even if unauthorized access occurs, the data remains indecipherable.
- **Employee Training:** All staff members undergo data security training to foster awareness and compliance with security protocols.
- **Incident Response Plan:** Midland has a comprehensive incident response plan in place to address any data breaches or security incidents promptly and effectively. Requesting Entities (REs) and Authentication Service Agencies (ASAs) must host their servers for Aadhaar authentication requests within data centers located in India. ASAs are required to establish dual redundant, secure leased lines or MPLS connections with the Authority's data centers, following the specified procedures and security guidelines. REs must access the authentication facility through an ASA using appropriate license keys over a secure network, as directed by the Authority. Both REs and ASAs must comply with all applicable regulations, security policies, standards, and guidelines issued by the Authority.

(Refer to Compendium of regulations, circulars and guidelines- Section1- Aadhaar regulations- Point no. 22.)



4.2 Access Control:

Midland employs stringent access control measures to restrict data access to authorized personnel only. This involves:

- **Role-Based Access:** Access permissions are assigned based on job roles, ensuring that employees can only access data necessary for their responsibilities.
- **Multi-Factor Authentication (MFA):** To enhance security, MFA is employed for accessing sensitive systems and data.
- **Access Logs:** Midland maintains logs of data access activities, allowing for monitoring and auditing of access patterns.

Access rights and privileges to information facilities handling UIDAI data must be reviewed quarterly, with the review reports retained for audit purposes. Access to information facilities handling UIDAI data (e.g., authentication applications, servers, audit logs, source code, and security infrastructure) shall be restricted to authorized individuals. AUA/KUA employees with such access must follow the principle of least privilege and ensure they log out after completing their sessions. Workstations, servers, and network devices must have locking mechanisms, and applications should implement auto-logout features after a period of inactivity (15 minutes or as defined by AUA/KUA policy).

(Refer to Compendium of regulations, circulars and guidelines-Information security policy- 2.6-Access Control)

4.3 Data Encryption:

Midland applies encryption techniques to protect data both in transit and at rest. This includes:

- **TLS/SSL Encryption:** Data transmitted over networks is encrypted using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols.
- **Data-at-Rest Encryption:** Sensitive data stored in databases or on physical media is encrypted to prevent unauthorized access in case of breaches.

For composite terminal devices with biometric readers that lack embedded encryption software, the communication between the biometric reader and the device handling encryption must be secured against all security threats and attacks.

(Refer to Compendium of regulations, circulars and guidelines-Information security policy- 2.11)

4.4 Data Retention and Deletion:

Midland adheres to data retention policies in compliance with the DPDP Act. This involves:

- **Retention Periods:** Data is retained only for the necessary period as defined by applicable laws and regulations.
- **Data Deletion:** Personal data is promptly deleted when it is no longer required for its original purpose or when individuals request their data to be erased.

4.5 Third-Party Data Processors:



When third-party data processors are engaged or will be engaged, Midland shall/will ensures they also adhere to data protection standards. This involves:

- **Due Diligence:** Midland conducts assessments of third-party data processors to ensure they meet security and compliance requirements.
- **Data Processing Agreements:** Contracts with third parties stipulate data protection obligations and compliance with the DPDP Act.

4.6 International Data Transfers:

In the event of international data transfers, Midland will comply with the DPDP Act's provisions on cross-border data transfers:

- **Central Government Notification:** Data transfers will be made to countries or territories which would be approved by the Central Government. If a jurisdiction is not approved, transfers will not occur.
- **Sectoral Regulations:** Midland would adhere to any additional laws or regulations that provide higher standards for data transfers.

These data protection measures are crucial to ensure that personal data is handled responsibly and securely, aligning with the principles of the DPDP Act and respecting individuals' rights to privacy and data protection.

4. Privacy Rights of Individuals

Midland Microfin is fully committed to upholding these privacy rights as mandated by the DPDP Act and will provide the necessary support and information for individuals to exercise these rights effectively.

5.1 Right to Information

Individuals have the right to receive clear, transparent, and easily understandable information about how Midland processes their personal data. This includes details on what data is collected, the purposes of processing, the lawful basis for processing, how long the data will be retained, and who it may be shared with. This information ensures that individuals are fully informed about the use of their data.

5.2 Right to Access

Individuals have the right to access their personal data held by Midland. This means they can request information about whether or not their data is being processed and, if so, obtain a copy of the data. Midland will provide this information in a structured, commonly used, and machine-readable format to ensure accessibility.



5.3 Right to Rectification

If individuals believe that the personal data Midland holds about them is inaccurate or incomplete, they have the right to request corrections. Midland will promptly assess such requests and make necessary amendments to ensure data accuracy.

5.4 Right to Erasure (Right to Be Forgotten)

Under certain circumstances, individuals have the right to request the deletion or removal of their personal data. This right allows individuals to have their data erased when there is no compelling reason for its continued processing.

5.5 Right to Restrict Processing

Individuals can request the restriction of processing their personal data. This means that Midland can continue to store the data but not process it further. This right is typically exercised when the accuracy of the data is contested, or the processing is unlawful.

5.6 Right to Data Portability

Individuals have the right to obtain and reuse their personal data for their purposes across different services. Midland will provide this data in a structured, commonly used, and machine-readable format, allowing individuals to transfer it to other data controllers.

5.7 Right to Object

Individuals can object to the processing of their personal data for certain purposes, such as direct marketing. Midland will stop processing the data unless there are compelling legitimate grounds for processing that override the individual's interests, rights, and freedoms.

5.8 Right to Appeal Automated Decision Making

When Midland uses automated decision-making processes that significantly affect individuals, they have the right to request human intervention, express their point of view, and challenge the decision. Midland will ensure that individuals have the opportunity to appeal and seek a review of such automated decisions.

5. Consent and Withdrawal

In adherence to stringent data protection regulations, Midland Microfin places paramount importance on the processes of obtaining and withdrawing consent concerning individuals' personal data.

6.1 Obtaining Consent



Midland, as a responsible data fiduciary, ensures that consent is obtained from individuals before processing their personal data. The consent process is designed to be clear, transparent, and easily understandable. Individuals are provided with detailed information about the purposes of data processing, the types of data involved, and any third parties with whom the data may be shared. Consent is obtained through clear affirmative actions, ensuring that it is freely given, specific, informed, unconditional, and unambiguous.

Requesting entities must obtain the consent of the Aadhaar number holder for authentication after providing the required information under Regulation 5. This consent should be obtained in physical or, preferably, electronic form, with logs or records maintained as specified by the Authority.

(Refer to Compendium of regulations, circulars and guidelines-Aadhaar authentication regulation-Point no.6)

6.2 Withdrawal of Consent

Individuals have the right to withdraw their consent at any time. Midland respects this right and has established mechanisms for individuals to easily withdraw their consent. The process for withdrawing consent is as simple as giving it, ensuring that individuals have control over their data at all times.

6.3 Consequences of Withdrawing Consent

When an individual withdraws their consent for data processing, Midland will cease processing their data for the specified purpose. It's important to note that the withdrawal of consent does not affect the legality of data processing that occurred before the withdrawal. Midland will promptly stop processing the data and, if there is no other lawful basis for processing, will delete the data as per data retention policies. This ensures that individuals have control over their data and how it is used.

6. Data Sharing

Midland's commitment to data protection means that all parties with whom the organisation share the personal data of the individual(s), these organisations must strictly adhere to agreements designed to safeguard individuals' information and uphold privacy rights, with a focus on preventing any breach of these agreements. A KUA may store e-KYC data in encrypted form with the Aadhaar holder's consent and share it with other agencies for specified purposes, provided separate consent is obtained from the Aadhaar holder for each instance of sharing.

(Refer to Compendium of regulations, circulars and guidelines-Aadhaar authentication regulation-Point no.16(1))

7.1 Disclosure to Third Parties



Midland may, in compliance with applicable data protection laws and regulations, disclose individuals' personal data to third parties under certain circumstances. These third parties, such as business partners, vendors, or service providers, enter into agreements with Midland, committing to abide by strict data protection standards, ensuring the security and confidentiality of the shared information, and preventing any breach of these agreements. The Aadhaar holder can revoke their consent at any time for a KUA to store or share their e-KYC data. Upon revocation, the KUA must delete the data and stop any further sharing.

(Refer to Compendium of regulations, circulars and guidelines-Aadhaar authentication regulation-Point no.16(5))

7.2 Sharing for Legal Compliance

Midland may be obligated to share personal data with law enforcement agencies, regulatory bodies, or other authorities to comply with legal requirements, court orders, or to respond to legal requests. In such cases, they ensure that the recipients of this data are bound by agreements to handle the information in a manner that upholds data protection principles, individual privacy rights, and ensures no breach of these agreements.

7.3 Sharing with Service Providers

Midland may engage third-party service providers to assist in various operations, including data processing, customer support, or technology services. These service providers are carefully selected and contractually bound to adhere to strict data protection agreements. They are only provided with access to the personal data necessary to perform their specific functions while abiding by the agreements in place, ensuring no breach of these agreements.

7.4 Sharing with Credit Bureaus:

In certain cases, Midland may share individuals' credit-related information with authorized credit bureaus or credit reporting agencies as required by law. These credit bureaus are bound by agreements that ensure the responsible handling and protection of the shared data, preventing any breach of these agreements. This practice is essential for assessing creditworthiness and maintaining compliance with regulatory standards.

7. Cookies and Tracking

Midland encourages users to review its Cookie Policy for more detailed information on the types of cookies used, their purposes, and instructions on how to manage cookie preferences effectively. By offering these options, Midland aims to empower individuals to make informed choices about their online privacy and tracking preferences.



8.1 Use of Cookies

Midland's website and online services may utilize cookies and similar tracking technologies to enhance user experiences. Cookies are small text files that are stored on an individual's device when they visit a website. These cookies serve various purposes, including improving website functionality, remembering user preferences, and analysing website traffic patterns. By using cookies, Midland aims to provide a more personalized and efficient online experience for its users. These cookies do not typically contain personally identifiable information, and individuals can manage their cookie preferences, as explained in section 8.3.

8.2 Third-Party Cookies

In addition to first-party cookies set by Midland's website, there may be third-party cookies placed by external service providers and partners. These third-party cookies are utilized for purposes such as analytics, advertising, and social media integration. Third-party cookies may collect data on browsing behaviour and interests to provide targeted content and ads. It's important to note that third-party cookies are subject to the privacy policies and practices of the respective third parties. Midland does not control these cookies, and individuals should review the privacy policies of these third parties to understand how their data is handled.

8.3 Managing Cookie Preferences:

Midland respects individuals' preferences regarding cookies and provides options for managing them. Users can typically adjust their cookie preferences through the website's cookie consent banner or browser settings. This allows individuals to accept, reject, or delete cookies based on their preferences. It's important to note that disabling certain cookies may impact the functionality of the website or limit access to specific features.

8. Grievance Redressal

Midland is dedicated to ensuring that individuals' concerns are addressed promptly and fairly. The organization values feedback from its users and is committed to continuous improvement in its data protection practices based on the insights gained through grievance redressal.

9.1 Contact Information for Grievances

Midland is committed to addressing any concerns or grievances Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes related to the processing of personal data promptly and effectively. Individuals who wish to raise a grievance or have inquiries regarding their privacy rights and



data protection can reach out to Midland's dedicated Grievance Redressal Team. Contact details for the Grievance Redressal Officer are provided below:

- **Name of Grievance Redressal Officer:**
- **Mailing Address:**
 Midland Microfin Ltd
 The AXIS, BMC Chowk,
 G.T. Road, Jalandhar – 144 001
 Punjab. INDIA
 Tel : +91 181 5076000
Email: grievance.redressal@midlandmicrofin.com

Midland would ensure that all communications related to grievances are handled with the utmost confidentiality and professionalism.

(Refer to Compendium of regulations, circulars and guidelines-Aadhaar authentication regulation-Point no.18(4))

9.2 Procedure for Handling Complaints

Midland Microfin has established a well-defined procedure for handling complaints and grievances related to data protection and privacy matters. Here's an overview of the complaint handling process:

- ❖ **Submission of Complaint:** Individuals who have a grievance related to their personal data can submit their complaint or concern to the Grievance Redressal Team using the provided contact information.
- ❖ **Acknowledgment:** Upon receiving a complaint, Midland will acknowledge the receipt of the grievance promptly, typically within business days.
- ❖ **Investigation:** Midland will initiate an internal investigation into the matter raised in the complaint. This investigation will be carried out by trained and qualified personnel to ensure a fair and impartial assessment.
- ❖ **Resolution:** Midland is committed to resolving complaints in a timely manner. Depending on the complexity of the issue, the resolution may take some time. However, Midland will keep the complainant informed of the progress and expected timelines.
- ❖ **Communication of Outcome:** Once the investigation is complete, Midland will communicate the outcome to the complainant. If the complaint is found to be valid, Midland will take appropriate measures to address the issue, which may include



corrective actions, policy adjustments, or further communication with the complainant.

- ❖ **Escalation:** If the complainant is not satisfied with the resolution provided by Midland, they have the option to escalate the matter to relevant data protection authorities as per the provisions of applicable data protection laws.

9. Updates and Changes

10.1 Policy Updates

Midland may periodically update this Privacy Policy to reflect changes in data protection laws, industry best practices, or modifications to its data processing practices. These updates are essential to ensure that individuals' personal data is handled with the utmost care and in compliance with applicable regulations.

10.2 Notification of Changes

Midland is dedicated to ensuring that individuals are informed about any significant changes to this Privacy Policy brought about by new government regulations or legal requirements. Here's how Midland handles such notifications:

- **Notification Timing:** Midland will notify users of any material changes to the Privacy Policy at least days before the changes take effect, except where required by law to provide immediate notice.
- **Notification Methods:** Midland will communicate policy updates through various means, which may include:
 - **Email:** Users who have provided their email addresses will receive an email outlining the changes to the Privacy Policy.
 - **Website Notification:** A notice of the policy changes will be prominently displayed on Midland's website, ensuring that users are aware of the updates.
 - **In-App Notifications:** If applicable, users may receive notifications within Midland's mobile or web applications.
 - **Other Appropriate Channels:** Midland may use other suitable channels to communicate policy changes, depending on the available means of reaching users (messages, calls from the back office, what sup etc).
- **Policy Accessibility:** The updated Privacy Policy will be made accessible to users at all times on Midland's website or through other relevant platforms.



Midland encourages users to review the updated Privacy Policy carefully to understand how their personal data may be affected by any changes. Users will be provided with the opportunity to express their preferences regarding the use of their data following significant policy updates. If users do not agree with the changes, they may have the option to discontinue using Midland's services, as outlined in the "Withdrawal of Consent" **section 6.2 & 6.3** of this Privacy Policy.

10. Copyright Notice

The content, design, and materials contained in this Privacy Policy, including but not limited to text, logos, and any other elements, are protected by applicable copyright laws. All rights to these materials are either owned by Midland or used under appropriate licenses or permissions.

11.1 Copyright Information

Individuals visiting or accessing this Privacy Policy are granted a limited, non-exclusive, and non-transferable right to view, download, or print the contents solely for personal and non-commercial purposes, provided that they do not modify or remove any copyright, trademark, or other proprietary notices. Any other use of the materials on this website or associated platforms, including but not limited to reproduction, distribution, display, or transmission, is strictly prohibited without prior written consent from Midland.

For any inquiries or requests regarding the use of materials from this Privacy Policy, individuals may contact Midland through the provided contact information. Unauthorized use of these materials may violate copyright, trademark, and other applicable laws and could result in legal action. © 2023 Midland. All rights reserved.

11. Exclusions and Limitations

Midland Microfin strives to provide accurate and up-to-date information in this Privacy Policy. However, the Company makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability concerning the information, products, services, or related graphics contained herein. Any reliance an individual places on such information is strictly at their own risk.

12.1 Limitations of Liability



In no event shall the Company be liable for any direct, indirect, consequential, or any other damages arising out of or in connection with the use of this Privacy Policy or the information contained within. This includes, but is not limited to, loss of data, loss of profits, business interruption, or any other pecuniary loss.

The Company makes no warranties or representations, either express or implied, that the use of this Privacy Policy will not infringe any proprietary rights or copyrights of third parties.

The information presented in this Privacy Policy is subject to change without notice. While the Company endeavours to keep the information up-to-date and correct, they make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability concerning the website or the information, products, services, or related graphics contained herein.

Through this Privacy Policy, individuals may be able to access other websites that are not under the control of the Company. The inclusion of any links does not necessarily imply a recommendation or endorsement of the views expressed within them. The Company has no control over the nature, content, and availability of those sites. Therefore, they cannot be responsible for the protection and privacy of any information individuals provide while visiting such sites, and such sites are not governed by this Privacy Policy.

By using this Privacy Policy, individuals acknowledge that they have read, understood, and agreed to the exclusions and limitations of liability contained herein. If they do not agree with these terms, they should not use or access this Privacy Policy.

Please refer to the "Contact Information" **section 9.1** of this Privacy Policy for inquiries or clarifications regarding these limitations of liability.

Note: This section is a general disclaimer and should be reviewed and customized as needed to accurately reflect the specific limitations and exclusions applicable to the company's privacy policy.

12. General Data Protection Regulation (GDPR) Compliance

"Midland Microfin acknowledges the significance of adhering to the General Data Protection Regulation (GDPR) to protect the rights and freedoms of individuals residing in India concerning their personal data."



The GDPR sets out fundamental principles that guide the processing of personal data. These principles serve as the foundation for how the Company handles and protects personal data:

- **Lawfulness, Fairness, and Transparency:** The Company would ensure that personal data is processed lawfully, fairly, and transparently. This means that individuals are informed about how their data is used, and their data is processed in a manner that aligns with applicable data protection laws.
- **Purpose Limitation:** Personal data which will be collected for specified, explicit, and legitimate purposes. The Company shall not process personal data in ways that are incompatible with these purposes.
- **Data Minimization:** The Company will only collect the personal data that is necessary for the purposes for which it is processed. Unnecessary or excessive data will not be collected.
- **Accuracy:** The Company would take reasonable steps to ensure that personal data is accurate and up to date. Inaccurate data is corrected or erased without delay.
- **Storage Limitation:** Personal data would be retained only for as long as necessary for the purposes for which it was collected. When data is no longer needed, it is securely deleted or anonymized.
- **Integrity and Confidentiality:** The Company would implement appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, or damage. Confidentiality and integrity of personal data are maintained.
- **Accountability:** The Company shall be accountable for complying with the GDPR's principles. This includes implementing data protection policies, conducting data protection impact assessments, and maintaining records of processing activities.

13. Do & Don't

Midland Microfin is dedicated to maintaining the confidentiality of your information in collaboration with our customers and stakeholders. The company's "Do & Don't" guidelines outline best practices for safeguarding your privacy and ensuring data security.

Do's:

1. **Educate Yourself:** Take the time to understand the privacy policies of websites and apps you use regularly. Being informed about how your data is collected and used is crucial.
2. **Use Strong Passwords:** Use unique and complex passwords for your online accounts. Consider using a reputable password manager to help you keep track of them.



3. **Enable Two-Factor Authentication (2FA):** Whenever possible, enable 2FA for your online accounts. This provides an extra layer of security.
4. **Keep Software Updated:** Regularly update your operating system, applications, and antivirus software to protect against known vulnerabilities.
5. **Be Cautious with Personal Information:** Be mindful of what personal information you share online. Avoid sharing sensitive data like your Social Security number, financial details, or home address unless necessary.
6. **Use Encryption:** Whenever possible, use encrypted communication methods, especially when sending sensitive information.
7. **Share Data Securely:** It is encouraged to share data through secure and approved channels to protect sensitive information.
8. **Use VPN for Added Security:** When accessing company resources remotely, using a VPN (Virtual Private Network) is recommended for enhanced security.
9. **Seek Prior Approval for Downloads:** Before downloading any applications or software, obtain prior approval to ensure they meet security standards.
10. **Do Regularly Review Privacy Settings:** Periodically review and update the privacy settings on your social media accounts and other online platforms to control what information is shared.

Don'ts:

1. **Don't Overshare on social media:** Avoid sharing excessive personal information, such as your exact location, travel plans, or daily routines, on social media platforms.
2. **Don't Click on Suspicious Links:** Be cautious when clicking on links or downloading attachments from unknown sources. These could contain malware or phishing attempts.
3. **Don't Ignore Software Updates:** Neglecting software updates can leave your devices vulnerable to security breaches.
4. **Don't Use Public Wi-Fi for Sensitive Activities:** Avoid conducting sensitive transactions or accessing sensitive accounts while on public Wi-Fi networks, as they may not be secure.
5. **Don't Fall for Phishing Scams:** Be sceptical of unsolicited emails or messages asking for personal or financial information. Verify the source before sharing any sensitive data.
6. **Don't Use Weak Passwords:** Avoid using easily guessable passwords like "123456" or "password." These are easy targets for hackers.
7. **Don't Ignore Privacy Policies:** Take the time to read and understand the privacy policies of the services you use. Ignoring them may lead to unintended data sharing.
8. **Don't Leave Devices Unattended:** Lock or log out of your devices when not in use to prevent unauthorized access.



9. **Avoid Unapproved Downloads:** Do not download applications or software without obtaining the necessary approvals, as unauthorized downloads may pose security risks.
10. **Refrain from Connecting to Third Parties:** Avoid connecting to third-party services or networks that have not been approved by Midland Microfin, as this could compromise data security.
11. **Exercise Caution with Email Sharing:** Exercise caution when sharing data over email, especially sensitive information, and use secure channels whenever possible to minimize risks.



1. Introduction

1.1 Purpose of the Privacy Policy:

The Privacy Policy of Midland Microfin serves a critical purpose in safeguarding user privacy. It is designed to inform users about how their personal information is collected, used, processed, and protected. By clearly defining these practices, it aims to create transparency and trust between the organization and its users.

1.2 Scope of the Privacy Policy: This policy applies comprehensively to all interactions users have with Midland Microfin's services and website. It covers the entire spectrum of data-related activities, ensuring that users are fully aware of how their data is handled.

- **1.3 Definitions:** To eliminate any ambiguity, Midland Microfin provides explicit definitions of key terms used throughout the policy. Definitions, including those for "personal data," "processing," and "data subject," are included to ensure that users have a clear understanding of the terminology used.

2. Information We Collect

- **2.1 Data Collection Methods:** Midland Microfin employs various methods to collect user data, including direct user submissions, automated data collection tools (such as cookies and analytics), and data received from trusted third parties. These methods are explained in detail to give users a comprehensive view of how their data is gathered.
- **2.2 Types of Personal Data Collected:** The company collects a wide range of personal data, which may include but is not limited to names, contact information, financial details, demographic information, and transaction history. Users are provided with specific examples of the types of data that may be collected.
- **2.3 Collection of Sensitive Information:** Midland Microfin takes privacy seriously and only collects sensitive data, such as financial or health information, when it is absolutely necessary and with explicit user consent. This section outlines the purpose of collecting such sensitive data and the stringent safeguards in place to protect it.
- **2.4 Collection from Minors:** To address the unique challenges of collecting data from minors, this section emphasizes the importance of parental consent and describes the additional measures taken to protect the data of individuals below the legal age.

3. How We Use Your Information

- **3.1 Purpose of Data Processing:** This section elucidates the underlying reasons for processing user data, which range from delivering services to improving products and enhancing the overall user experience. By providing insight into the purposes, Midland Microfin aims to instill confidence in users.



- *3.2 Legal Basis for Data Processing:* Users are informed about the legal grounds on which their personal data is processed. This may include user consent, contractual obligations, and the legitimate interests of the organization, ensuring full transparency in data processing activities.
- *3.3 Data Processing for Marketing:* Midland Microfin acknowledges the importance of marketing in its operations. This section explains how user data may be employed for marketing purposes, including sending promotional materials, offers, and updates.
- *3.4 Automated Decision-Making:* In cases where automated decision-making processes are utilized, such as credit assessments, this section provides clear information about how these processes work and their potential impact on users.

4. Data Protection Measures

- *4.1 Data Security:* Midland Microfin leaves no room for compromise when it comes to data security. This section delves into the comprehensive measures in place to protect user data, including encryption protocols, access controls, routine security assessments, and employee training programs.
- *4.2 Access Control:* The policy emphasizes that access to user data is strictly limited to authorized personnel within the organization, bolstering user confidence in the confidentiality of their information.
- *4.3 Data Encryption:* Users are reassured by the company's use of state-of-the-art encryption technologies to safeguard data during transmission and storage.
- *4.4 Data Retention and Deletion:* Midland Microfin is committed to data retention practices that align with regulatory requirements. This section provides users with clear information on how long their data is retained and the criteria used for its eventual deletion.
- *4.5 Third-Party Data Processors:* In cases where third parties are involved in data processing, this section clarifies their roles and responsibilities in maintaining data privacy and security.
- *4.6 International Data Transfers:* For users concerned about cross-border data transfers, this section outlines the safeguards in place to protect data during international transmission, ensuring that user data remains secure and compliant with relevant regulations.

5. Your Privacy Rights

- *5.1 Right to Information:* Users have a fundamental right to know how their data is being processed. This section empowers users to request detailed information about the processing of their data.
- *5.2 Right to Access:* Midland Microfin respects users' rights to access their personal data. This section explains the process for users to request access to their data and obtain copies.



- *5.3 Right to Rectification:* Users can request corrections to inaccurate or incomplete data, and this policy provides a straightforward procedure for rectification.
- *5.4 Right to Erasure (Right to Be Forgotten):* The company respects users' right to have their data deleted under certain circumstances. Users are informed of the conditions and procedures for exercising this right.
- *5.5 Right to Restrict Processing:* In specific situations, users can request restrictions on the processing of their data. This section outlines the criteria and steps to take when invoking this right.
- *5.6 Right to Data Portability:* Users have the right to receive their data in a structured, machine-readable format. This section provides details on how to make such requests.
- *5.7 Right to Object:* Users can object to the processing of their data, especially in cases of direct marketing. The policy explains the process for submitting objections.
- *5.8 Right to Appeal Automated Decision Making:* In scenarios involving automated decision-making processes, users retain the right to appeal such decisions. This section provides clarity on the process for lodging appeals and having decisions reviewed.

6. Consent and Withdrawal

- *6.1 Obtaining Consent:* Midland Microfin emphasizes the significance of informed and freely given consent for data processing activities. This section explains how consent is obtained and the importance of user understanding.
- *6.2 Withdrawal of Consent:* Users are informed of their right to withdraw consent at any time. The policy clarifies the straightforward process for withdrawing consent.
- *6.3 Consequences of Withdrawing Consent:* To ensure transparency, users are informed of the potential consequences of withdrawing consent, which may include limitations on certain services.

7. Data Sharing

- *7.1 Disclosure to Third Parties:* Users are provided with a detailed understanding of the circumstances under which their data may be shared with third parties, including the purposes of such disclosure.
- *7.2 Sharing for Legal Compliance:* Midland Microfin is committed to adhering to legal requirements. This section outlines the situations in which data may be shared to comply with legal obligations or respond to legal requests.
- *7.3 Sharing with Service Providers:* The policy clearly communicates that data may be shared with trusted service providers who assist in delivering products and services. Users are reassured about the security of such data sharing.
- *7.4 Sharing with Credit Bureaus:* To provide users with transparency regarding credit assessments, this section explains how data may be shared with credit bureaus for assessment purposes.



8. Cookies and Tracking

- *8.1 Use of Cookies:* The policy is transparent about the use of cookies and similar tracking technologies on Midland Microfin's website. It explains the purposes of these technologies and how they enhance the user experience.
- *8.2 Third-Party Cookies:* In cases where third-party cookies are employed, users are provided with detailed information about these cookies and their specific purposes.
- *8.3 Managing Cookie Preferences:* To empower users to make informed choices about cookies, this section offers clear instructions on managing cookie preferences and settings.

9. Grievance Redressal

- *9.1 Contact Information for Grievances:* Midland Microfin places a strong emphasis on addressing user concerns. Users are provided with the necessary contact information to raise privacy-related grievances.
- *9.2 Procedure for Handling Complaints:* The company is committed to handling user complaints efficiently and fairly. This section outlines the procedure for users to follow when lodging complaints about data handling practices.

10. Updates and Changes

- *10.1 Policy Updates:* Users are informed that the privacy policy may be updated from time to time to reflect changes in data handling practices or regulatory requirements. The policy emphasizes the importance of reviewing updates.
- *10.2 Notification of Changes:* To ensure transparency, the policy describes how users will be notified of any changes to the policy, such as through website notifications or email alerts.

11. Copyright Notice

- *11.1 Copyright Information:* The policy includes essential information about the copyright of the content on the website. It informs users about the permitted and prohibited uses of copyrighted material.

12. Exclusions and Limitations

- *12.1 Limitations of Liability:* Midland Microfin acknowledges that, despite robust security measures, data breaches or unauthorized access may occur. This section outlines the limitations of liability concerning such events and emphasizes the importance of user data protection practices.

13. General Data Protection Regulation (GDPR) Compliance

- *13.1 GDPR Principles:* Users are informed about the fundamental principles of GDPR compliance, including lawful, fair, and transparent data processing. The policy highlights the commitment to these principles.
- *13.2 GDPR Rights and Compliance:* The policy ensures users understand their rights under GDPR and how Midland Microfin complies with these rights, including lawful data processing, transparent communication, and robust data protection practices.



14. Contact Information

- *14.1 Contact Details:* Users are provided with clear and comprehensive contact information to reach out to Midland Microfin for any privacy-related inquiries, concerns, or requests. This includes email addresses, phone numbers, and physical addresses.

By providing this detailed information, Midland Microfin aims to ensure that users are fully informed about its data privacy practices, rights, and how to exercise them, thereby fostering trust and transparency in its data handling processes.

15. Review and Regulatory Supremacy

This Policy shall be reviewed at least once in every year or earlier, as may be required, to incorporate changes arising from applicable laws, regulatory guidelines, supervisory instructions, or evolving business and operational requirements.

In the event of any inconsistency between the provisions of this Policy and any applicable law, regulation, circular, guideline, or direction issued by a statutory or regulatory authority (including the Reserve Bank of India), such law or regulatory requirement shall prevail to the extent of such inconsistency, and this Policy shall be deemed to be amended accordingly.