Privacy policy

1.0 PURPOSE

This privacy policy describes the management of personal information that Manappuram Asset Finance Ltd (Here after refers as MAAFIN) or its representative collects from or about the employee/customer/vendor and describes how it is used. The company collects and uses personal data in a reasonable and lawful manner. The Company may amend these rules from time to time.

2.0 SCOPE

2.1 MAAFIN does collect your personal information for a variety of regulatory and business purposes. These include, but are not limited to:

1. Verify your identity
2. Complete transaction of Products and Services
3. Respond to the request for any service/assistance
4. Perform market analysis, market research, business and operational analysis
5. Provide, maintain and improve our Product and Services
6. Anticipate and resolve issues and concerns with our Product and Services
7. Ensure adherence to legal and regulatory requirements for prevention and detections of frauds and crimes

3.0 DEFINITIONS

3.1 Personal Information -The term 'Personal Information' applies to any information that is used to identify/contact an employee/customer/vendor for business purposes. This includes an individual's name, fathers name, mothers name, spouse name, current and previous address, date of birth, contact details, details, occupation, professional memberships etc. not limited to any information as required by the Company. In the normal course of business activities, the company will collect personal information but under certain exceptional circumstances Company may collect Sensitive Personnel

Information (SPI) also. MAAFIN and its authorized third parties may collect, store, process following types of Sensitive Personal Information such as password, financial information (details of Bank account, credit card, debit card, or other payment instrument details), biometric information, physiological information for providing our products, services and for use of our website. We may also hold information related to your utilization of our services which may include your call details, your browsing history on our website, location details and additional information provided by you while using our services.

3.2 Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 defines Sensitive Personal Information. Sensitive Personal data or information of a person means such personal information which consist of any information relating to:

1. password;
2. financial information such as Bank account or credit card or debit card or other payment instrument details;
3. physical or physiological and mental health condition
4. sexual orientation
5. medical records and history
6. Biometric information
7. any detail relating to the above clauses as provided to body corporate for providing service; and
8. 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 Right to Information Act, 2005or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purpose of these rules.

4.0 POLICY

4.1 Collection of Personal Information

4.1.1MAAFIN may collects various types of personal information about an employee/client/vendor under various circumstances. They are collected from

- Resumes and/or applications;
- References and interview notes;
- Proof of Identity (photo ID cards, Passport etc.)
- Certificates of educational/ professional qualifications.
- Photographs and video;
- Letters of offer and acceptance of employment;
- Mandatory policy acknowledgment sign-off sheets;
- Information relating to payroll, pay cheque deposit information, and other related information;
- Forms relating to the application for, or in respect of changes to, employee health and welfare benefits; including, short and long term disability, medical and dental care; and
- Beneficiary and emergency contact information.

4.1.2 In addition personal information also includes name, address, date of birth, phone number, mailing address, credit card information, and any other relevant information necessary to company's business purposes. The company may also collect personal information of employees/clients from third parties, if required for business.

4.1.3 MAAFIN may at its discretion employ, contract or include third parties external to itself for strategic, tactical and operational purposes. Such agencies though external to MAAFIN, will always be entities which are covered by contractual agreements. These agreements in turn include MAAFIN`s guidelines to the management, treatment and secrecy of personal information. We may transfer your personal information or other information collected, stored, processed by us to any other entity or organization located in India only in case it is necessary for providing services to you or if you have

consented (at the time of collection of information) to the same. This may also include sharing of aggregated information with them in order for them to understand our environment and consequently, provide you with better services. While sharing your personal information with third parties, adequate measures shall be taken to ensure that reasonable security practices are followed at the third party. We may obtain your consent for sharing your personal information in several ways, such as in writing, online, through "click-through" agreements; orally, including through interactive voice response; or when your consent is part of the terms and conditions pursuant to which we provide you service. We, however assure you that MAAFIN does not disclose your personal information to unaffiliated third parties (parties outside MAAFIN corporate network and its Strategic and Business Partners) which could lead to invasion of your privacy.

4.1.4 MAAFIN may also share your personal information with Government agencies or other authorized law enforcement agencies (LEAs) mandated under law to obtain such information for the purpose of verification of identity or for prevention, detection, investigation including but not limited to cyber incidents, prosecution, and punishment of offences.

4.2 Use of Personal Information

4.2.1 The personal information collected is used in a manner that is compatible with the purpose for which it is collected. Such uses may include:

- Determining employment eligibility in case of an applicant for job (verification of reference and qualification);
- Establishing, managing and terminating employment relationships with the company in case of an employee;
- Such other reasonable purposes as required by the Company for customers/vendors or employees.

4.3 Disclosure of Personal Information

4.3.1 Personal Information may be shared or disclosed by the company either internally or externally with third parties/Clients for the purpose for which it was collected. An individual can withdraw consent at any time, subject to

legal and contractual restrictions. MAAFIN will inform the implications of such withdrawal.

4.3.2 Further, personal information may be disclosed under the following circumstances:

- Where required by applicable law or legal processes;
- Where permitted by law without individual's consent;
- Where it is necessary to protect the rights and property (including intellectual property) and all other confidential information of the company;
- Where situation arise to protect the safety of an individual or a group;
- Where it forms part of the daily reporting activities to employees and other persons.

4.4 Security of Personal Information

4.4.1 The company is responsible to secure the personal information it holds regardless of the form in which the information is stored. The company has taken appropriate measures to prevent any loss, misuse, unauthorized access, disclosure, or modification of Personal Information. Our security practices and procedures limit access to personal information on need-only basis. Further, our employees are bound by Confidentiality Policies which obligate them to protect the confidentiality of personal information. We take adequate steps to ensure that our third parties adopt reasonable level of security practices and procedures to ensure security of personal information. We may retain your personal information for as long as required to provide you with services or if otherwise required under any law. When we dispose of your personal information, we use reasonable procedures to erase it or render it unreadable (for example, shredding documents and wiping electronic media).

4.5 Reasonable Security Practices and Procedures

4.5.1 We have put in place appropriate technical, organizational and security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.
4.5.2 We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so

4.6 Right of Access to Personal Information

4.6.1 The company allows employees/clients to access personal information only on their requests. If any personal information needs to be updated or verified, it shall be informed to the HR Manager/CIO.
4.6.2 In cases where an employee/client is restricted access to personal information; the company will explain the reasons for the lack of access, except where prohibited by law. Additionally, personal information may be destroyed or erased, in accordance with the company's record retention policies.

4.7 Retention

4.7.1 Personal data is kept in active files or systems only as long as needed to meet the purposes for which it was collected or as required by contractual agreement, by law or regulation, or, where applicable for the appropriate statute of limitations period. Records will be periodically reviewed and archived or properly disposed of according to the company’s record retention policy. Personal data may be archived to meet legal requirements, for research purposes or to facilitate long-term storage.

4.8 Disclaimer

4.8.1 Every effort has been made to ensure that the information stated by the individual is correct and up to date, however, Company does not provide any warranty as to the completeness or accuracy of the information and, subject to applicable laws, does not accept any liability for damages of any kind resulting from any unauthorized access or for any advertisement published regarding. employee/customers Personnel information.

4.9 Complaint Resolution

4.9.1 Any employee/customer who has a concern about the collection, use or disclosure of the individual's personal data can directly file a complaint before the HR Manager /CIO. The company will investigate and ensure appropriate resolution. The company will make reasonable efforts to maintain confidentiality regarding the employee/customers concern.