# MANAPPURAM FINANCE LIMITED (MAFIL)

## POLICY ON DIGITAL PERSONAL DATA PROTECTION

| **Version Control** | | |
|---|---|---|
| **Version Number** | **Description** | **Date** |
| Version 1 | Creation | 06.03.2025 |
| Version 1.1 | Modified | 01-04-2026 |

| | |
|---|---|
| **Effective Date** | 09-05-2025 |
| **Reviewed Date** | 27-04-2026 |
| **Next Review Date** | 08-05-2027 |
| **Policy Owner** | Data Protection Department / DPO |
| **Prepared By** | DPO |
| **Modified By** | DPO - Sajith C |
| **Reviewed by** | CRO |
| **Approved By** | Board Of Directors |

# Contents

**MAFIL'S DATA PROTECTION POLICY:**

**ENSURING COMPLIANCE WITH THE DIGITAL PERSONAL DATA PROTECTION ACT 2023**

## INTRODUCTION

The Digital Personal Data Protection Act 2023 (hereinafter referred to as the "DPDP Act") received Presidential assent and was officially gazetted, becoming enforceable as of 11 August 2023. The DPDP Act is an important legislation aimed at establishing comprehensive standards for the responsible handling of digital personal data. Its primary objective is to strike a delicate balance between safeguarding individuals' rights to privacy and imposing legal obligations on entities acting as data fiduciaries, including MAFIL.

Under the DPDP Act, MAFIL assumes a critical role as a data fiduciary, defined as entities, whether acting independently or in conjunction with others, that determine the purpose and means of processing personal data. This broad definition encompasses various forms of data, including but not limited to information related to MAFIL's customers, employees, and other relevant stakeholders.

The DPDP Act explicitly outlines the duties and obligatiAons of data fiduciaries, providing clear parameters within which personal data must be managed. Compliance with these regulations is imperative for MAFIL to uphold the standards of lawful data processing.

Simultaneously, the legislation enshrines the rights of individuals, referred to as Data Principals, who are essentially data subjects to whom the personal data pertains. The DPDP Act ensures that Data Principals have specific rights safeguarded under the law, emphasizing the necessity for transparency and fairness in the processing of their personal information.

## 1. KEY TERMINOLOGIES

### A. Consent

MAFIL should seek consent, which is a voluntary, specific, informed, and unambiguous indication of the Data Principal's wishes.

### B. Consent Manager

A Consent Manager, as defined by the DPDP Act, is an individual or entity registered with the Data Protection Board of India (DPBI) and acts as a singular point of contact facilitating Data Principals in giving, managing, reviewing, and withdrawing their consent through an accessible, transparent, and interoperable platform. This entity may be a third-party company, duly registered with the DPBI, obligated to adhere to the DPDP Act's stipulations concerning data privacy and security.

**C. Notice**

As per the DPDP Act, a notice is required when processing is based on consent. MAFIL, as a Data Fiduciary, should provide clear, itemised, and simple language details of personal data, its purpose, and the manner in which Data Principals can exercise their rights. Data Principals have the option to access information in English or any of the 22 languages (as per the Eight Schedule of the Indian Constitution).

The notice should include information on filing complaints before the Board. For processing activities with pre-existing consent, MAFIL should issue a fresh privacy notice meeting the above requirements.

D. Personal Data
Personal data refers to any information about an individual associated with MAFIL as a customer / Employee, which can identify them or is related to their identity.

E. Digital personal data
Digital personal data refers to personal information that is stored or processed in digital format.

**F. Data Fiduciary**

Data Fiduciaries, such as MAFIL, are organizations or individuals deciding the collection, processing, and purposes of data. MAFIL should explicitly acknowledge and accept its responsibilities as a Data Fiduciary under the DPDP Act.

**G. Significant Data Fiduciary**

Significant Data Fiduciaries, processing large volumes of sensitive data, will be designated by the Government. In the event of MAFIL being designated as Significant Data Fiduciary, additional obligations as per the DPDP Act should be duly complied with.

**H. Principal**

"Data Principals" include individuals like MAFIL's customers, employees, and stakeholders. For minors (<18 years), consent from Parents/Guardians is mandatory, and MAFIL should ensures compliance with the prohibition on behavioural monitoring and targeted advertising for children.

**I. Data Processor**

Data processors, such as MAFIL's service providers, process data on behalf of Data Fiduciaries based on their instructions. MAFIL is required to ensure its data processors (service providers) comply with the DPDP Act.

**J. Legitimate Uses**

Certain "legitimate uses" recognised under the Act do not require separate consent. This includes data voluntarily provided, data collected for legal obligations, responding to medical emergencies, maintaining public order, ensuring safety, employment-related purposes, and activities in public interest. MAFIL should periodically review processes falling under legitimate uses to ensure continued DPDP Act compliance.

## 2. APPLICABILITY & SCOPE OF DPDP ACT

### A. Applicability Within India and Beyond:

i. The Digital Data Protection Act (DPDP) of 2023 applies to the processing of digital personal data within the territorial boundaries of India. This includes data collected both online and offline, which is subsequently digitized. Furthermore, the DPDP Act extends its jurisdiction to the processing of digital personal data that occurs outside the territory of India, specifically in situations where goods or services are provided to data principals within the boundaries of India.

ii. Any transfer of digital personal data outside the territorial boundaries of India by MAFIL, whether to a third party or an affiliate, shall strictly adhere to the DPDP Act's stipulated safeguards and mechanisms. MAFIL should ensure that such transfers align with its commitment to protecting the rights of data principals.

### B. Exempted Personal Data:

i. Personal data processed by individuals for personal or domestic purposes is exempted from the provisions of the DPDP Act.

ii. Personal data voluntarily made publicly available by the data principal, whether by choice or due to legal obligation, is excluded from the DPDP Act. This exemption encompasses personal data publicly disclosed on social media and other prominent platforms. However, it is crucial to emphasize that this exclusion does not absolve MAFIL of its obligations in managing personal

data obtained through alternative means, such as behavioural monitoring or direct messaging.

### C. Exceptions:

The DPDP Act outlines certain processing activities that are exempted from specific obligations. These exceptions include:

i. Enforcement of legal rights or claims within MAFIL's legal framework.
ii. Performance of judicial or regulatory duties by a court or other relevant bodies applicable to MAFIL.
iii. Prevention or investigation of offenses related to MAFIL's operations.
iv. Performance of a contract with a foreign entity involving personal data of data principals outside of India, within the context of MAFIL's contractual obligations.
v. Mergers and acquisitions or reconstruction of the organization approved by a judicial body.
vi. Debt enforcement within MAFIL's financial operations

## 3. GROUNDS OF PROCESSING PERSONAL DATA

### A. Consent

i. A valid consent under the DPDP Act is a foundational prerequisite for processing personal data. MAFIL is obligated to procure valid consent from the data principal. It is important to note that such consent must be freely given, specific, informed, unconditional, and unambiguous, establishing a clear affirmative action by the Data Principal. Notably, the inclusion of the term "unconditional" implies that legislators intend to confine consent to the primary purpose for which it is collected. Consequently, combining consent for secondary purposes may render it conditional.

ii. MAFIL must ensure that when processing a minor's personal data, consent from their lawful guardian is mandatory. However, it is crucial to acknowledge that consent is not absolute under the DPDP Act. This provision necessitates MAFIL to afford Data Principals the right to withdraw their consent at any point during the processing

### B. Legitimate Use

i. Various bases for processing personal data, such as legal obligations, medical emergencies, and employment, fall under legitimate uses. When personal data is processed under legitimate uses, excluding cases of voluntary provision, Data Principals relinquish certain rights. Specifically, in

such instances, the Data Principals do not retain the right to erase, correct, or access their personal data, nor can they withdraw their consent.

ii. MAFIL is mandated to be diligent in identifying and adhering to legitimate uses, ensuring transparency and communication with Data Principals regarding the potential limitations on their rights when personal data is processed under such grounds.

**C. Privacy Notice**

i. In compliance with the DPDP Act, MAFIL is obligated to provide a privacy notice, particularly when the ground of processing is based on consent. MAFIL is required to furnish comprehensive details concerning personal data, specifying the purpose of processing, and outlining the manner in which Data Principals can exercise their rights under the DPDP Act.

ii. MAFIL has an obligation to make the privacy notice available in either English or any of the twenty-two languages specified in the Eighth Schedule of the Constitution, ensuring accessibility to a diverse range of Data Principals. Additionally, MAFIL is required to inform Data Principals about the procedure for filing a complaint before the Board, as an integral part of the notice.

iii. In cases where consent has been obtained before the enactment of the law, MAFIL is obligated to provide a renewed privacy notice, incorporating the aforementioned requirements to ensure continued compliance with the DPDP Act.

## 4. Securing personal data across all software systems.

I. Scope of Data Processing: Mention that all software, handling personal data must comply with the DPDP Act.
II. Third-Party & Vendor Compliance: Any third-party software or cloud service used must have Data Protection Agreements (DPAs).
III. Data Security Measures: Specify encryption, access control, and breach notification as mandatory features for any software handling personal data.
IV. Cross-Border Data Transfers: If software transfers data outside India, compliance with DPDP Act's transfer regulations is required.
V. Any software, handling personal data must be approved by the Data Protection Officer before implementation.

## 5. Data Privacy

### 5.1 General Obligations of MAFIL

### A. Implement Comprehensive Technical and Organizational Measures:

MAFIL shall implement and maintain robust, continuously updated, and internationally recognized technical and organizational measures to safeguard the security and confidentiality of personal data. These measures shall include, but are not limited to:

i. Data encryption: Encrypt personal data both at rest and in transit using industry-standard encryption algorithms.

ii. Access controls: Implement granular access controls to restrict access to personal data to authorized personnel only.

iii. Data loss prevention mechanisms: Deploy data loss prevention (DLP) technologies to prevent unauthorized access, use, disclosure, modification, or destruction of personal data.

iv. Regular vulnerability assessments: Conduct regular vulnerability assessments and penetration testing to identify and address potential security weaknesses.

v. Employee training on data privacy practices: Provide comprehensive training to all employees on data privacy practices, including data security awareness, incident reporting procedures, and compliance with the DPDP Act.

### B. Determine Legal Grounds and Obtain Consent:

MAFIL shall adhere to the principles of data minimization and purpose limitation, ensuring that personal data is collected only for specified, explicit, and legitimate purposes. MAFIL shall identify the legal grounds for processing personal data in accordance with the DPDP Act, such as consent, contractual necessity, legal obligations, or vital interests. MAFIL shall obtain explicit, informed, and verifiable consent from Data Principals where required under the DPDP Act. The consent mechanism shall be clear, transparent, and easy to withdraw.

### C. Provide Privacy Notice:

MAFIL shall provide a clear, concise, and easily accessible privacy notice to Data Principals at the time of data collection or when seeking consent. The privacy notice shall outline the following information:

i. The purpose and scope of data processing, including the specific categories of personal data to be collected and processed.

ii. The retention period for personal data.

iii. The Data Principal's rights under the DPDP Act, including the right to access, rectification, erasure, restriction of processing, data portability, and objection to processing.

iv. The contact information for the Data Protection Officer.

v. Any information about the transfer of personal data to third parties or countries outside India.

**5.2 Facilitate Exercise of Rights:**

A. MAFIL shall establish and maintain an easily accessible and user-friendly mechanism allowing Data Principals to exercise their rights in relation to their personal data. These rights include the right to:

i. Access: Obtain access to their personal data and information about the processing of their personal data.

ii. Rectification: Request the rectification of inaccurate personal data.

iii. Erasure: Request the erasure of their personal data, subject to certain exceptions.

iv. Restriction of processing: Request the restriction of the processing of their personal data.

v. Data portability: Receive their personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller without hindrance.

vi. Object to processing: Object to the processing of their personal data on grounds relating to their particular situation. MAFIL shall respond to Data Principal requests promptly and within the timelines specified in the DPDP Act. If MAFIL is unable to comply with a request, it shall provide the Data Principal with an explanation of the reasons for its refusal.

**5.3 Grievance Redressal Mechanism:**

i. MAFIL shall establish and maintain an effective, responsive, and accessible grievance redressal mechanism to address queries, concerns, and complaints raised by Data Principals regarding their personal data.

ii. The grievance redressal mechanism should be transparent, impartial, and free of charge. MAFIL shall designate a Data Protection Officer (DPO) to oversee the grievance redressal process and ensure timely resolution of

grievances. The DPO shall be readily available to receive and address Data Principal grievances.

**5.4 Irrecoverable Deletion of Personal Data:**

i. MAFIL shall implement a procedure for the irreversible deletion of personal data upon request from the Data Principal, unless such deletion is incompatible with or hinders the performance of a contract to which the Data Principal is a party, or where the processing is necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims.

ii. MAFIL shall ensure that the deletion of personal data is complete and irretrievable and shall not retain any copies or backups of the deleted data, unless otherwise required by the RBI or other applicable laws, regulations, or directives in place to retain or store the data for a specified period.

**5.5 Breach Management Policy:**

**A.** To effectively mitigate the risks associated with data breaches, MAFIL shall establish and maintain a comprehensive breach management policy that encompasses the following key aspects:

i. Identification and Reporting: MAFIL shall implement mechanisms for timely identification and reporting of data breaches, including establishing clear criteria for determining what constitutes a breach.

ii. Investigation: Upon identifying a potential breach, MAFIL shall promptly conduct a thorough investigation to determine the nature, extent, and cause of the breach.

iii. Notification: MAFIL shall notify the Data Protection Board (DPB) and affected Data Principals without undue delay, following the timelines specified in the DPDP Act. The notification should provide a clear description of the breach, the affected personal data, potential consequences, and remedial measures taken.

iv. Remediation: MAFIL shall take appropriate remedial measures to address the breach, including implementing corrective actions to prevent future occurrences and providing support to affected individuals.

**B.** BREACH NOTIFICATION

i. Timing of Breach Notification

The Digital Personal Data Protection Act, 2023 (DPDP Act) does not explicitly specify a timeframe for notifying the Data Protection Board (DPB) and affected data principals in the event of a personal data breach. However, the Act mandates that such notification must be made "without undue delay." This implies that the notification should be made as soon as practicable after becoming aware of the breach.

Considering the potential harm that a personal data breach can cause to individuals, MAFIL should strive to notify the Data Protection Board (DPB) and affected data principals within the existing security incident notification timeline of six hours prescribed by the Computer Emergency Response Team (CERT).

ii. Contents of Breach Notification

The breach notification to the DPB and affected data principals should provide a clear and concise description of the following:

- The nature of the personal data breach, including the type of personal data involved and the estimated number of affected data principals.
- The date and time of the breach, or the timeframe within which it is believed to have occurred.
- The potential risks or harm that may arise from the breach for affected data principals.
- The measures taken by MAFIL to contain the breach, mitigate its impact, and prevent future occurrences.
- Recommendations for steps that affected data principals can take to protect themselves from potential harm arising from the breach.

iii. Communication Channels for Breach Notification

MAFIL should establish clear communication channels for notifying the DPB and affected data principals in the event of a personal data breach with in 72 hours. The specific channels used may vary depending on the circumstances of the breach and the nature of the data involved. However, MAFIL should prioritize the use of secure and reliable communication methods to protect the confidentiality of personal data.

iv. Documentation and Record-Keeping

MAFIL should maintain detailed documentation and records of all personal data breaches, including the breach notification process. These records should be readily accessible to the DPB for purposes of investigation and compliance audits.

v. Training and Awareness

MAFIL should provide regular training and awareness programs to its employees on the DPDP Act's breach notification requirements and the company's internal breach notification procedures. This will ensure that employees are equipped to promptly identify, report, and respond to personal data breaches.

### 5.6 Retention & Deletion

MAFIL is obligated to delete personal data when it is no longer necessary for the purpose for which it was collected, or when the Data Principal withdraws their consent, whichever is earlier. Additionally, if the Data Principal does not interact with MAFIL or utilize its services for a certain period as prescribed by the Data Protection Board of India (DPDB), the retention period shall be deemed to have expired, and MAFIL would be required to erase such personal data.

A. Determination Of Retention Periods

MAFIL will determine the appropriate retention period for personal data based on the following factors:

i. The purpose for which the data was collected:
MAFIL will retain personal data only for the specific purpose or purposes for which it was collected. Once the purpose has been fulfilled, the data should be deleted unless there is a valid legal or contractual basis for retention.

ii. The legal or contractual obligations that MAFIL is subject to:
MAFIL may be required to retain certain personal data in order to comply with laws or regulations, such as record-keeping requirements mandated by the Reserve Bank of India (RBI). These retention periods will supersede any general retention periods set by MAFIL.

iii. The legitimate interests pursued by MAFIL:
MAFIL may retain personal data for its legitimate interests, such as preventing fraud, detecting and investigating security breaches, or maintaining accurate records for internal audits. However, the retention periods set forth in DPDP Act will supersede any general retention periods set by MAFIL.

iv. Sectoral laws and regulations:
In addition to general data protection laws, MAFIL may also be subject to sectoral laws and regulations that mandate different retention timelines.

For example, RBI may require NBFCs to retain certain customer records for a specified period.

B. Procedures For Deletion Of Personal Data

MAFIL will implement secure procedures for the deletion of personal data, including:

i. Physical destruction of paper records:
Paper records containing personal data should be securely shredded or incinerated to prevent unauthorized access.

ii. Secure erasure of electronic records:
Electronic records containing personal data should be securely erased using appropriate software tools to ensure that the data cannot be recovered.

iii. De-identification of personal data:
Personal data may be de-identified by removing any information that can directly identify an individual. De-identified data can still be used for certain purposes, such as research or analytics, but it poses a lower risk to data privacy.

iv. Notification to relevant MAFIL departments and third-party processors:
MAFIL should notify all relevant departments and third-party processors that handle personal data when personal data is deleted. This will ensure that the data is deleted from all systems and that there are no conflicting retention policies.

v. MAFIL will regularly review and update its retention and deletion policy to reflect changes in applicable laws and regulations, technological advancements, and business practices.

**5.7 Valid Contracts with Data Processors:**

MAFIL shall enter into legally binding and comprehensive contracts with Data Processors, ensuring adherence to key obligations under the DPDP Act. These obligations include:

A. Processing Personal Data Only in Accordance with MAFIL's Instructions and for Specified Purposes

i. Data Processors shall only process personal data in accordance with MAFIL's written instructions and for the specified purposes communicated by

MAFIL. Data Processors shall not process personal data for any other purpose unless authorized in writing by MAFIL or required by law.

ii. MAFIL shall ensure that its instructions to Data Processors are clear, specific, and consistent with the DPDP Act. MAFIL shall also provide Data Processors with all necessary information to enable them to comply with their obligations under the DPDP Act.

B. Implementing Appropriate Technical and Organizational Measures to Safeguard Personal Data

i. Data Processors shall implement appropriate technical and organizational measures to safeguard personal data against unauthorized or unlawful processing and accidental loss, destruction, or damage. These measures shall include, but are not limited to, access controls, encryption, data backup procedures, data minimization practices, and regular risk assessments.

ii. MAFIL shall regularly audit Data Processors' data security practices to ensure that they are adequate and effective. MAFIL shall also provide Data Processors with training on data security awareness and best practices.

C. Notifying MAFIL Promptly of Any Data Breaches or Potential Risks to Personal Data

i. Data Processors shall promptly notify MAFIL of any data breaches or potential risks to personal data that come to their attention. Data Processors shall provide MAFIL with all relevant information about the data breach or potential risk, including the nature of the breach, the affected personal data, and the potential impact on Data Principals.

ii. MAFIL shall have a documented data breach response plan in place to effectively respond to data breaches. The plan should include procedures for notifying Data Principals, relevant authorities, and MAFIL's management.

D. Cooperating with MAFIL in Responding to Requests from Data Principals

i. Data Processors shall cooperate with MAFIL in responding to requests from Data Principals regarding their personal data. This includes providing Data Principals with access to their personal data, rectifying inaccurate personal data, erasing personal data upon request, and restricting the processing of personal data in certain circumstances.

ii. MAFIL shall provide Data Processors with clear and timely instructions on how to respond to Data Principals' requests. MAFIL shall also provide Data

Processors with access to the personal data necessary to comply with Data Principals' requests.

E. Deleting or Returning Personal Data at the End of the Processing Agreement

i. Data Processors shall delete or return all personal data to MAFIL upon termination of the processing agreement, unless otherwise instructed in writing by MAFIL or required by law. Data Processors shall certify to MAFIL that they have deleted or returned all personal data upon termination of the processing agreement.

ii. MAFIL shall maintain a record of all data processing agreements and the personal data processed under each agreement. This record will be used to ensure that personal data is properly deleted or returned at the end of the processing agreement.

F. Regular Review and Update of Data Processing Agreements

i. MAFIL shall regularly review and update its data processing agreements to reflect changes in the law or data processing practices. MAFIL shall also review data processing agreements when there is a change in the scope of processing, the category of personal data being processed, or the Data Processor.

ii. MAFIL shall keep Data Processors informed of any changes to the DPDP Act or MAFIL's data processing practices. MAFIL shall also provide Data Processors with the opportunity to review and update their data processing agreements in light of these changes.

G. Consequences of Non-Compliance

i. MAFIL should ensure that Data Processors comply with all applicable requirements of the DPDP Act and shall take appropriate action in the event of any non-compliance. MAFIL should take necessary action against Data Processors who fail to comply with their obligations under the DPDP Act. MAFIL may also terminate its DPAs with Data Processors who fail to comply with their obligations

## 6. OBLIGATIONS OF SIGNIFICANT DATA FIDUCIARY

Significant Data Fiduciaries that process large volumes of sensitive data will be designated by the Government. However, the Central Government has not yet notified the criteria for designating Significant Data Fiduciaries. Therefore, in the event that MAFIL is designated as a Significant Data Fiduciary, it must duly comply

with the additional obligations set forth in the DPDP Act. These additional obligations set forth below are designed to ensure that MAFIL implements enhanced measures to protect the personal data of its customers and other data subjects.

**A. Appointment of a Data Protection Officer (DPO)**

In the event that MAFIL is designated as an SDF, MAFIL shall appoint a Data Protection Officer (DPO) who shall be based in India. The DPO shall be a qualified and experienced professional with expertise in data protection law and practices. The DPO shall have the following responsibilities:

i. Overseeing MAFIL's compliance with the DPDP Act and ensuring that MAFIL's data processing practices align with the principles laid out in the Act.

ii. Acting as a point of contact for data subjects and regulatory authorities, addressing their queries, complaints, and representations regarding data privacy matters.

iii. Advising MAFIL's senior management on data protection matters, providing expert guidance on data privacy risks, compliance strategies, and best practices.

iv. Conducting training and awareness programs on data protection for MAFIL employees, ensuring that all employees understand their roles and responsibilities in protecting personal data.

The DPO shall have direct access to MAFIL's senior management and shall be provided with the necessary resources to effectively discharge his or her responsibilities.

**B. Assign a Data Owner in each department**

**Responsibilities of Data Owners**

To strengthen data governance and compliance, each department must designate a Data Owner responsible for managing and protecting personal data.

**Data Owner is accountable for the following actions.**

I. Ensure proper data handling in their respective departments.
II. Act as a liaison between their department and the DPO.
III. Ensure data collection, processing, and storage comply with DPDP regulations.
IV. Maintain an updated inventory of personal data processed within their

department.

V. Classify department data based on personal, sensitive, critical.

VI. Responsible for unauthorized access, sharing or modifications of personal data.

VII. Ensure employees and customers can exercise the data rights (access, correction, deletion).

VIII. Report data breaches or unauthorized access to the DPO immediately.

**C. Appointment of an Independent Data Auditor**

MAFIL shall appoint an independent data auditor to conduct periodic data audits. The data auditor shall be a qualified and experienced professional with expertise in data security and privacy auditing. The data auditor shall have the following responsibilities:

i. Assessing MAFIL's compliance with the DPDP Act, evaluating whether MAFIL's data processing practices adhere to the Act's requirements and principles.

ii. Identifying and reporting on data protection risks, analyzing MAFIL's data processing activities to detect potential vulnerabilities and threats to data privacy.

iii. Making recommendations for improving MAFIL's data protection practices, providing actionable insights to strengthen MAFIL's data protection posture and mitigate identified risks.

**D. Appointment of an Independent Data Auditor**

MAFIL shall appoint an independent data auditor to conduct periodic data audits. The data auditor shall be a qualified and experienced professional with expertise in data security and privacy auditing. The data auditor shall have the following responsibilities:

iv. Assessing MAFIL's compliance with the DPDP Act, evaluating whether MAFIL's data processing practices adhere to the Act's requirements and principles.

v. Identifying and reporting on data protection risks, analyzing MAFIL's data processing activities to detect potential vulnerabilities and threats to data privacy.

vi. Making recommendations for improving MAFIL's data protection practices, providing actionable insights to strengthen MAFIL's data protection posture and mitigate identified risks.

MAFIL shall provide the data auditor with access to all relevant data, systems, and personnel to conduct a comprehensive and thorough audit.

**E. Conduct of Data Protection Impact Assessments (DPIAs)**

MAFIL shall conduct Data Protection Impact Assessments (DPIAs) for all high-risk data processing activities. A DPIA is a systematic process that identifies and assesses the potential risks to data subjects' rights and freedoms as a result of data processing activities.

MAFIL should consider the following factors when determining whether a data processing activity is high-risk:

i. The nature, scope, and context of the data processing activity.

ii. The sensitivity of the personal data being processed.

iii. The potential impact on data subjects' rights and freedoms.

MAFIL shall document the results of DPIAs and implement appropriate measures to mitigate identified risks.

**F. Additional Measures**

In addition to the aforementioned obligations, MAFIL should adopt other measures consistent with the DPDP Act, including:

i. Establishing a comprehensive data governance framework: MAFIL shall develop and implement a comprehensive data governance framework that outlines clear policies and procedures for the collection, storage, processing, use, and disclosure of personal data. The data governance framework shall be aligned with the principles of data minimization, purpose limitation, data accuracy, storage limitation, integrity, confidentiality, and accountability.

ii. Implementing robust data security measures: MAFIL shall implement industry-standard security protocols and practices to protect personal data from unauthorized access, breaches, and cyberattacks. These measures shall include technical safeguards, such as encryption, access controls, and intrusion detection systems, as well as organizational safeguards, such as data classification, data loss prevention, and incident response procedures.

iii. Providing data subjects with transparent and easily accessible information: MAFIL shall provide data subjects with clear and concise information about how their personal data is being collected, used, and disclosed. This information shall be provided in a readily accessible format and shall be easy to understand.

iv. Establishing a mechanism for handling data subject requests: MAFIL shall establish a mechanism for promptly and effectively responding to data subject requests for access, rectification, erasure, or restriction of processing of their personal data. MAFIL shall provide clear and concise information about the process for submitting data subject requests and shall ensure that requests are handled in a timely and efficient manner.

v. Continuous Monitoring and Review: MAFIL shall continuously monitor and review its data protection practices to ensure that they remain effective and compliant with the DPDP Act. MAFIL shall regularly evaluate and update its data protection policies, procedures, and security measures to adapt to evolving data privacy risks and regulatory requirements.

## 7. RIGHTS OF DATA PRINCIPAL

MAFIL should acknowledge and respect the rights of Data Principals under the Digital Personal Data Protection Act, 2023 (DPDP Act). MAFIL is committed to providing Data Principals with clear, transparent, and accessible information about their personal data and how it is being processed. MAFIL should implement and maintain appropriate measures to ensure that Data Principals can exercise their rights effectively.

i. Right to Withdraw Consent

Data Principals have the right to withdraw their consent to the processing of their personal data at any time. This right can be exercised by contacting MAFIL's Data Protection Officer (DPO) or through MAFIL's designated consent management mechanism. Upon receiving a withdrawal of consent, MAFIL should cease processing the respective Data Principal's personal data for the specified purpose(s) to the extent feasible. However, it is important to note that withdrawal of consent may not be possible in certain circumstances, such as when processing is necessary for the performance of a contract or for compliance with a legal obligation.

ii. Right to Grievance Redressal

Data Principals have the right to file a grievance with MAFIL if they believe

that their personal data has been processed in violation of the DPDP Act. MAFIL has established a comprehensive grievance redressal mechanism to address such grievances promptly and effectively. Data Principals can file a grievance by contacting MAFIL's DPO or through MAFIL's designated grievance redressal mechanism. MAFIL should acknowledge the receipt of a grievance and should provide a substantive response within a reasonable timeframe, in accordance with the DPDP Act. If the Data Principal is not satisfied with the response, they can escalate the matter to the Data Protection Board of India (DPBI).

iii. Right to Access Information

Data Principals have the right to access their personal data and to obtain information about how it is being processed. This information includes the purpose of processing, the categories of personal data being processed, the identities of any third parties to whom the personal data has been disclosed, and the retention period for the personal data. Data Principals can request access to their personal data by contacting MAFIL's DPO. MAFIL should provide the requested information within a reasonable timeframe, as stipulated in the DPDP Act or its rules.

iv. Right to Nominate

Data Principals have the right to nominate a representative to exercise their rights on their behalf in the event of their death or incapacity. The nomination should be made in writing and should specify the rights that the representative is authorized to exercise. The nominated representative will have the same rights as the Data Principal, and MAFIL should acknowledge and respect those rights.

v. Right to Correction and Erasure of Personal Data

Data Principals have the right to request MAFIL to correct any inaccurate or incomplete personal data. Data Principals also have the right to request MAFIL to erase their personal data in certain circumstances, such as when the personal data is no longer necessary for the purpose for which it was collected, when the Data Principal has withdrawn their consent, or when the processing of the personal data is in violation of the DPDP Act. Requests for correction or erasure of personal data should be made in writing and should specify the reasons for the request. MAFIL should respond to such requests promptly and in a manner consistent with the DPDP Act.

vi. Exceptions

The right to access, correction, and erasure of personal data is not absolute.

There are certain exceptions to these rights, such as when processing is necessary for the performance of a contract, for compliance with a legal obligation, or for the establishment, exercise, or defence of legal claims. Additionally, the right to erasure does not apply to personal data that has been anonymized or that is being processed for historical, scientific, or statistical purposes.

vii. Transparency and Accountability`

MAFIL shall be committed to transparency and accountability in its data processing practices. MAFIL should provide Data Principals with clear and accessible information about how their personal data is being collected, used, and shared. MAFIL should also maintain records of its data processing activities and should make those records available to Data Principals upon request.

**8. Data Inventory and Record of Processing Activities (RoPA)**

Manappuram Finance Limited shall maintain a comprehensive inventory of personal data processed across all departments. Each department shall maintain a Record of Processing Activities (RoPA), which shall include:

- Type of personal data collected
- Purpose of processing
- Legal basis for processing (consent / legitimate use / legal obligation)
- Retention period applicable
- Details of third-party vendors involved (if any)
- Data transfer details, including cross-border transfers (if applicable)

The Data Protection Department shall periodically review and update the data inventory to ensure compliance with the DPDP Act, 2023.

**9. Third-Party and Vendor Data Sharing Governance**

Personal data shall not be shared with any third-party vendor, consultant, service provider, or external entity without prior approval from the Data Protection Department.

Before sharing any personal data, the following requirements must be completed:

- Vendor risk assessment
- Execution of a Non-Disclosure Agreement (NDA) / MSA
- Execution of a Data Protection Agreement (DPA) / Inclusion of DPDP clauses in agreement. wherever applicable
- Confirmation of the purpose of data processing
- Approval from the Department Head and Data Protection Officer

Sharing of personal data based solely on an NDA / MSA shall not be permitted.

**10. Internal Approval Mechanism for Personal Data Processing**

Any new initiative, project, system implementation, or business process involving the collection, storage, or processing of personal data must be reviewed and approved by the Data Protection Department before implementation.

The approval process shall include:

- Department Head approval
- Data Protection Officer (DPO) approval
- Legal team approval (where required)
- Information Security / IT approval (where new systems or software are involved)

**11. Data Breach Identification and Internal Reporting**

All employees shall immediately report any suspected or confirmed personal data breach to the Information Security Team and the Data Protection Department.

The following internal timelines shall be followed:

- Employees must report incidents within 2 hours of identification
- Information Security Team shall conduct an initial assessment
- Data Protection Department shall evaluate the impact on data principals
- Escalation shall be made to senior management where required

Manappuram Finance Limited shall notify the Data Protection Board of India and affected data principals without undue delay, in accordance with the DPDP Act, 2023.

**12. Data Classification Requirements**

All personal data processed within the organization shall be classified based on sensitivity. The following classification categories shall be followed:

- Public Data
- Internal Data
- Confidential Data
- Personal Data
- Sensitive Personal Data
- Critical Personal Data (if applicable)

Each department shall ensure that personal data is handled, stored, and shared in accordance with the applicable classification level.

**13. Data Retention Governance**

Personal data shall be retained only for the period necessary to fulfil the purpose for which it was collected or as required under applicable laws and regulatory requirements.

Each department shall define and maintain a retention schedule for personal data handled by them. The Data Protection Department shall review the retention schedule periodically to ensure compliance with the DPDP Act, 2023.

## 14. Children's Personal Data Protection

Manappuram Finance Limited shall implement additional safeguards while processing children's personal data.

The following controls shall be implemented:

- Verifiable parental / Legal guardian consent shall be obtained before collecting children's personal data
- No behavioural tracking or profiling of children shall be carried out
- No targeted advertising shall be conducted using children's personal data
- Personal data of minors shall be processed only where it is strictly necessary and legally permitted

## 15. Accountability of Departments

Each department handling personal data shall be responsible for ensuring compliance with the DPDP Act, 2023 and the organization's data protection policies.

Department Heads shall ensure that:

- Employees handling personal data are properly trained
- Personal data is collected only for legitimate business purposes
- Personal data is not shared without authorization
- Data protection risks are reported to the Data Protection Department

## 16. FINES AND PENALTIES SPECIFIED IN DPDP ACT

### 16.1 Overview of the Tiered System of Fines and Penalties

The Digital Data Protection Act 2023 (DPDP Act) introduces a multi-tiered system of fines and penalties to deter non-compliance and incentivise organizations to implement robust data protection practices. The severity of the penalties is proportionate to the nature and impact of the violation. MAFIL will take all reasonable steps to avoid any fines or penalties under the DPDP Act.

### 16.2 Specific Violations and Corresponding Penalties

A. Failure to Implement Reasonable Security Safeguards:

i. Penalty: Up to Rs. 250 crore

ii. Applicable to: Data Processors and Data Fiduciaries (including MAFIL)

iii. Description: The DPDP Act mandates that organisations implement appropriate security measures to protect personal data from unauthorised access, use, disclosure, alteration, or destruction. Failure to implement such safeguards can result in severe penalties of up to Rs. 250 crore. This includes

implementing technical and organizational measures, such as data encryption, access controls, and regular security audits.

B. Failure to Notify the Data Protection Board and Affected Data Principals of Personal Data Breaches:

i. Penalty: Up to Rs. 200 crore

ii. Applicable to: Data Processors and Data Fiduciaries (including MAFIL)

iii. Description: In the event of a personal data breach, organizations are required to promptly notify the Data Protection Board of India (DPDB) and affected data principals. Failure to provide timely and accurate notifications can lead to substantial penalties of up to Rs. 200 crore. This includes identifying and reporting breaches within 72 hours of becoming aware of them, providing detailed information about the breach to affected individuals, and taking appropriate remedial measures to minimize the risk of harm.

C. Non-Fulfilment of Additional Obligations for Children's Data:

i. Penalty: Up to Rs. 200 crore

ii. Applicable to: Data Processors and Data Fiduciaries (including MAFIL)

iii. Description: The DPDP Act imposes stricter obligations for the collection and processing of children's personal data. Failure to comply with these additional requirements can result in significant penalties of up to Rs. 200 crore. This includes obtaining parental or guardian consent for data collection, implementing enhanced data security measures, and providing clear and accessible privacy notices to children and their parents or guardians.

D. Non-Fulfillment of Additional Obligations of Significant Data Fiduciaries:

i. Penalty: Up to Rs. 150 crore

ii. Applicable to: Significant Data Fiduciaries (SDFs)

iii. Description: SDFs are designated as entities that process large volumes of personal data or have significant social or economic impact. SDFs are subject to additional obligations under the DPDP Act. Failure to comply with these obligations can result in substantial penalties of up to Rs. 150 crore. This includes appointing a Data Protection Officer (DPO), conducting data protection impact assessments, and implementing data minimization practices.

E. Non-Compliance with Duties of Data Principals:

i. Penalty: Up to Rs. 10,000
ii. Applicable to: Data Principals

iii. Description: The DPDP Act outlines certain responsibilities for data principals, such as providing accurate information and cooperating with data processors and fiduciaries. Failure to comply with these duties can result in penalties of up to Rs. 10,000. This includes providing accurate and complete information when requested, withdrawing consent for data processing, and exercising their right to access, rectification, erasure, and portability of their personal data.

F. General Non-Compliance with DPDP Act Provisions:

i. Penalty: Up to Rs. 50 crore

ii. Applicable to: Any organization or individual in violation of the DPDP Act

iii. Description: This category encompasses any non-compliance with the DPDP Act not specifically covered by the above provisions. The severity of the penalty will depend on the nature and impact of the violation. This includes any failure to comply with the principles of data protection, data processing conditions, data transfer requirements, or any other provisions of the DPDP Act.

MAFIL should carefully review and understand the DPDP Act's provisions to ensure compliance and avoid potential penalties.

## 17. CONCLUSION

MAFIL is dedicated to safeguarding the privacy of its customers and stakeholders, upholding its reputation as a responsible and trustworthy organization. This legal policy outlines MAFIL's comprehensive approach to compliance with the Digital Data Protection Act 2023 (DPDP Act). This legal policy will undergo regular reviews and updates to align with any amendments to the DPDP Act or other relevant laws and regulations. MAFIL will conduct continuous training programs for its employees, focusing on the provisions of the DPDP Act and data protection practices, ensuring they are well-equipped to maintain the highest standards.

MAFIL's unwavering commitment to data protection is ingrained in its business operations, deeply rooted in its core values and ethical framework. This comprehensive legal policy serves as a robust framework for ensuring ongoing compliance with the DPDP Act and other applicable data protection laws and regulations, setting a benchmark for responsible data-handling practices within the industry.