PNB MetLife India Insurance Company Limited

Privacy Policy

Document Control:

Version No.	9.0
Policy Owner	Risk
Prepared By	Privacy Risk & InfoSec Risk Team
Reviewed By	Information Security Risk Committee (ISRMC) and Executive Risk Management Committee (ERMC)
Approved By	Board Asset Liability Management Risk (ALMR) Committee

Revision History:

Version	Date	Author	Review/ Comments
1.0	September 29, 2017	Ethics and Compliance	-
2.0	May 2019	Ethics and Compliance	Annual review - no change
3.0	May 15, 2020	Ethics and Compliance	Annual review - no change
4.0	May 25, 2021	Ethics and Compliance	Annual review - no key change
5.0	May 11, 2022	Ethics and Compliance	Annual review - no change
6.0	22 June 2023	Privacy Compliance Group (PCG)	1. Alignment with MetLife Privacy policy 2. Alignment to IRDAI Cyber Security released in April 2023
7.0	April 2024	Privacy Compliance Group (PCG)	No changes, annual review
8.0	Mar 2025	InfoSec Team	Alignment with MetLife Global Standard and Local Regulations
9.0	October 2025	Privacy & InfoSec Team	Aligned with stakeholder best practices. Privacy Risk Assessment process revised; RACI matrix added to define roles and responsibilities.

Contents

Preamble: PNB MetLife's Privacy Principles

PNB MetLife India Insurance Company's (PNB MetLife) Privacy Principles (the "Principles") establish the framework of this Policy and are values designed to inspire PNB MetLife employees, contractors and third-party to act consistently, ethically, and with due care when working with personal information. PNB MetLife employees are encouraged to follow these Principles based on applicable legal and regulatory requirements, or as otherwise deemed appropriate.

Principle 1: Respect privacy rights

Respecting the privacy rights of PNB MetLife's current, prospective and former employees, customers, prospective customers, business partners and other individuals whose Personal Data PNB MetLife processes in accordance with the data protection laws and relevant statutory and regulatory provisions.

Principle 2: Process personal data for a legitimate purpose

Personal data is collected in accordance with applicable data protection laws and relevant statutory and regulatory provisions, in a fair, lawful, and transparent manner. Such data is processed solely for the legitimate business purposes for which it was collected, and as clearly outlined in the PNB MetLife's privacy notices.

Principle 3: Protect Personal Data

Personal data will be protected in accordance with applicable data protection laws and relevant statutory and regulatory provisions. The PNB MetLife ensures data minimization by collecting only what is necessary for the intended purpose and implements appropriate technical and organizational safeguards across all personal data processing operations to uphold confidentiality, integrity, and accountability.

Principle 4: Maintain Accountability

The PNB MetLife remains accountable for monitoring and enforcing compliance with this Policy, as well as with applicable data protection laws and relevant statutory and regulatory provisions. In addition, the PNB MetLife is committed to fostering a strong culture of privacy awareness by providing regular privacy training and capacity-building initiatives across all levels of the organization.

Overview

A. Policy Statement (Scope and Purpose)

Customers, employees, contractors, third-party and business partners routinely entrust PNB MetLife with **Personal Information** ("PI"). They rely on PNB MetLife ("PNB MetLife") to protect and limit use of that information, as well as to respect their privacy in accordance with applicable data protection laws and relevant statutory and regulatory provisions. PNB MetLife is committed to meeting stakeholders' expectations by being a trusted steward of personal information provided to PNB MetLife. Protecting personal data is integral to maintaining customer trust and confidence. Any misuse of personal information or breach of data security can significantly undermine PNB MetLife's reputation for reliability and integrity, potentially leading to adverse financial and operational consequences.

Attention

Exceptions to this Policy must be escalated to **Ethics and Compliance** for review.
Any questions concerning this Policy should be directed to the PCG at askprivacy@pnbmetlife.com.

PNB MetLife's Privacy Policy ("Policy") establishes principles and adequate standards designed to mitigate privacy risks in accordance with applicable data protection laws and relevant statutory and regulatory provisions. Under this Policy, the Company will build and maintain robust controls over the **collection**, use, and protection of PII to comply with this Policy and in accordance with applicable data protection laws and relevant statutory and regulatory provisions. Company operations that involve processing personal information initially collected in another country may also be subject to the data protection laws and regulatory requirements of the jurisdiction where the data was originally collected along with the laws of the Land (Republic of India). Furthermore, Company may have contractual agreements that may impose obligations on it to protect certain sets of data, including personal information. Failure to comply with applicable legal requirements may damage the Company's reputation and expose the Company to legal and regulatory liabilities, including but not limited to fines, penalties and lawsuits.

The Company adheres to various management policies and practices as part of a commitment to protecting Personal Information. This document is intended to give clear and accessible information about those policies and practices. It explains the way PNB MetLife, and its employees, contractors and third party or vendors will collect, use, store, share, transmit, delete or otherwise process (collectively "process") Personal Information in accordance with applicable data protection laws and relevant statutory and regulatory provisions and its Privacy Principles.

What is Personal Information?

Personal information means information held in electronic or physical format that identifies or can identify an individual directly or indirectly and will include **Sensitive Personal Data or Information ("SPDI")**. Examples may include, but are not limited to:

- General identification and contact information (for example, name, e-mail address, phone numbers, and address)
- Identification numbers issued by government bodies or entities (for example, national identification number and passport number)
- Financial information and account details (for example, credit or other payment card numbers, income details and bank account numbers)
- Other sensitive personal information (for example, Physiological and mental health condition, health-related or medical information, racial or ethnic origin, sexual orientation, and political opinions).
- Technical identifiers (for example, user ID or username and password, device identification number, and geolocation); and
- Biometric Identifiers (for example, facial geometry, fingerprint, retina scan, and genetic information).
- Employee confidential information, such as compensation, performance, job history, etc.

Company employees must respect the confidentiality of and handle personal information in accordance with this Policy. For purposes of this Policy, the term **PI** will be used to refer to the personal information of PNB MetLife customers (including group participants), potential customers, employees, independent contractors, job applicants, business partners, and other third parties.

B. **Applicable Law**

Company and its employees, along with contractors and third-party are subject to, and must comply with, the Indian privacy laws, such as the Information Technology (Amendment) Act, 2008 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and other statutes as and when applicable, amended from time to time . This Policy shall comply with applicable laws and regulations. Where there are differences between the Policy and legal requirements, the appropriate legal framework should be applied based on jurisdiction and the intent of the regulation. Employees seeking clarification of this Policy's consistency with any applicable privacy law or regulation should contact the PCG at (askprivacy@pnbMetLife.com).

Attention

This Policy does not apply to workplace monitoring or electronic surveillance of PNB MetLife employee activities (for example, e-mail or Internet usage monitoring). Please contact the Law Department and/or Employee Relations for questions about applicable laws, regulations, and Company policies related to workplace privacy.

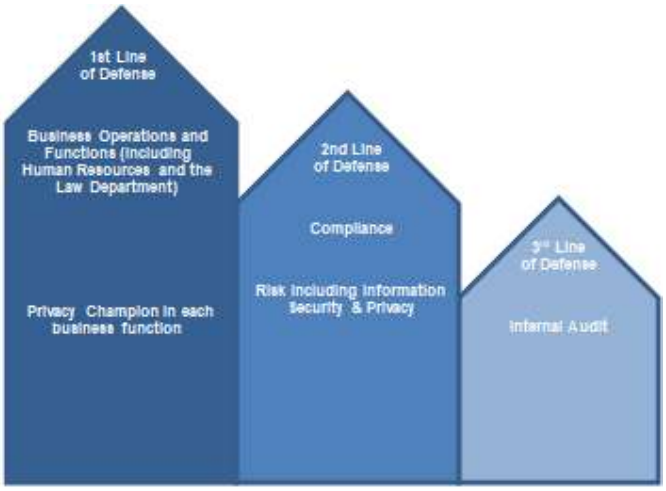
Who does this policy apply to?

This Policy applies to all employees, (collectively "employees"), contractors and third-party acting on behalf of PNB MetLife. Failure to comply may result in the erosion of customer confidence, reputational harm to the PNB MetLife, regulatory investigations, and penalties (including fines), lawsuits, and criminal penalties. Accordingly, employees, contractors and third-party who fail to comply with this Policy and/or applicable privacy laws and regulations may face disciplinary action, including but not limited to termination of employment with PNB MetLife. PNB MetLife will publish its privacy policy principles and relevant aspects of the policy on its website as required under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (hereinafter also referred as "Privacy Rules 2011) and other applicable data protection laws and relevant statutory and regulatory provisions, as may be applicable from time to time.

C. **Privacy risk management**

How are Privacy Risks and Controls Managed?

Every line of business serves as the first line of defense in managing day-to-day privacy risks. Privacy risks also are governed by the control functions, including Compliance, Risk Management, as the second line of defense and Internal Audit as the third line of defense. Roles and responsibilities with context to privacy risk management include:



First Line of Defence

Primary Responsibility and Accountability

- ✓ Owns and manages the risk and control environment.
- ✓ Identifies, assesses, mitigates, and approves risks.
- ✓ Conducts self-testing of controls in alignment with the Enterprise Risk Management (ERM) framework.

Second Line of Defence

Oversight and Advisory

- ✓ Advises business and functional areas
- ✓ Conducts independent monitoring and testing
- ✓ Collaborates with First Line of defence to agree on remediation plans and monitors their closure to ensure timely and effective resolution.

Third Line of Defence

Independent Assurance

- ✓ Validates the effectiveness and robustness of controls.
- ✓ Provides objective assessments of the overall risk and control environment.

D. Policy Requirements

The policy establishes the following requirements, which must be met to uphold the applicable data protection laws and relevant statutory and regulatory provisions, Privacy Principles. This includes embedding Personal Data protection principles in PNB MetLife's development and sourcing of technology (when that technology Processes Personal Data) and in the end-to-end design of systems and products, as applicable.

The minimum requirements and activities that shall be undertaken under this policy are as follows -

1. Privacy By Design: Incorporating privacy considerations in the design, implementation, operation and maintenance of products, processes, applications, and systems that Process or handle Personal Data, including when conducting mergers and acquisitions and by applying heightened standards for Sensitive Personal Data.

2. Privacy Risk Assessments: Performing a Privacy Risk Assessment ("PRA") of products, processes, applications, and systems as required under law.

3. Cross-Border Personal Data Transfers: Observing local requirements that may limit or restrict the transfer of Personal Data across country borders.

4. Privacy Notices and Data Subject Rights: Providing privacy notices with clear, accurate, and transparent language that describes the Personal Data Processing undertaken, intended business purpose(s), and where applicable, consent mechanisms for Individuals to exercise their privacy rights.

5. Retention of Personal Data: Retaining and disposing of Personal Data in accordance with PNB MetLife ILM Policy.

6. Safeguards: Implementing appropriate administrative, technical, physical, and operational measures designed to protect the confidentiality, integrity, and availability of Personal Data.

7. Personal Data Incidents: Escalating, reporting, containing, and assessing Personal Data Incidents in accordance with legal and regulatory obligations.

8. Other Data Transfers: Entering and updating written agreements so that data entrusted to PNB MetLife is contractually protected according to applicable PNB MetLife minimum standards when that data is shared with, handled, or processed by another party on PNB MetLife's behalf or transferred among MetLife legal entities. 9. 9, Personal Data Minimization and Retention - Data minimization, retention, and disposal of Personal Data follow PNB MetLife minimum data collection practices, retention and disposal policies, legal obligations, and legitimate business purposes.

10. Safeguards Requirements: PNB MetLife shall implement safeguard measures or controls under which personal information is protected from unauthorized access by the MetLife Entity, other MetLife Entities, and/or its Data Processors, Data Controllers and Third Parties.

11. Privacy Notice: Privacy notices shall describe the legitimate purpose for which customers data collected shall be processed.

12. Data Deletion: On specific data deletion or erasure requests received from the customers, PNB MetLife specific business functions shall ensure that the same is complied with and customer requests are abided except in cases where law or regulatory requirements prohibits.

E. Privacy Roles and Responsibilities

Management in the lines of business and first-line functions is responsible for implementing processes and controls in PNB MetLife operations that are designed to deter, detect, and prevent potential privacy risks. For purposes of this Policy, the term **business management** will be used to collectively refer to management in the lines of business and first-line functions.

- **PNB MetLife Data Protection Officer *(Applicability- post notification of DPDPA Rules)***

PNB MetLife Privacy Office will be headed by the PNB MetLife Second Line of Defense. The Data Protection Officer (DPO) will serve as the designated Privacy Officer for PNB MetLife. ***The DPO shall be appointed once the Rule framed therein are notified by the Government of India (GoI)***.

- **Privacy Compliance Group (PCG)**

The local PCG shall have representations from multiple functions to facilitate implementation of privacy policies and standards on the ground. PCG will also be involved in reviewing Privacy controls periodically. ***The PCG shall report to the Chief Risk Officer and the Data Protection Officer (as and when applicable).***

The PCG shall perform the following responsibilities -

- Facilitate and support Business Functions with implementation efforts.
- Seek Business Function feedback, where appropriate.
- Liaise with PCG to report on local implementation progress and provide local privacy training.
- Identification of local privacy requirements and imposing stricter requirements.
- Where applicable, drafting and maintaining local Policy and Standard and following the Privacy governance process for changes, amends, and exceptions.
- Monitoring and testing privacy controls.
- Where relevant, overseeing the closure of privacy policy issues.
- Design and make available online training module on the Policy and Standard

- **Business Functions**

The business functions shall perform the following responsibilities -

- Providing review of the Policy requirements as appropriate.
- Implementation of controls relating to Policy and Standard requirements and document evidence of compliance.
- Quality assurance conducted on privacy controls.
- Make staff available to attend or complete the required privacy training.
- Policy violations and issues arising out of quality assurance and/or monitoring and testing are reported, and appropriate mitigation is undertaken using the appropriate reporting tools.

- **Non- Financial Risk (NFR) Programme under Second Line of Defence**

The officer responsible for NFR Programme, is responsible for overseeing the controls management has in place to mitigate privacy risk through the Non-Financial Risk Testing and Monitoring. The function is also responsible for ensuring that:

(i) Policy is periodically reviewed and updated are in consultation with the legal department and basis the best practices observed from Industry including learnings from best practices of shareholder.

(ii) employees are familiar with applicable privacy laws;

(iii) the PNB MetLife maintains a robust privacy compliance program;

(iv) ongoing training is provided to senior management, key operating personnel, and other employees based on risk;

(v) employees are updated on any changes to the privacy compliance program and/or applicable regulatory requirements;

(vi) risk assessments are conducted in compliance with PNB MetLife's Compliance Risk Management Policy

(vii) Exception to this policy is duly reviewed by Chief Risk Officer.

- **Chief Risk Officer (CRO)**

On at least an annual basis, the Chief Risk Officer of PNB MetLife, or his or her designee, will provide a report to the Board ALMR Committee on any significant privacy risks and issues that may have been identified during the prior year across PNB MetLife's operations, as well the mitigation plans for these risks and issues.

- **Chief Information Security Officer (CISO)**

The Chief Information Security Officer (CISO) at PNB MetLife reports to the Chief Risk Officer and leads the Information/Cyber Security Program. The CISO supports the Privacy Officer in defining controls for protecting personally identifiable information, in line with the IT (Amendment) Acts of 2008 and 2011, and other applicable regulations. Responsibilities include:

- Enforcing information security policies and coordinating with internal teams and external agencies.
- Collaborating with IT and Security Operations to align security with business needs.
- Convening the Information Security Risk Management Committee (ISRMC) and proposing policies.
- Assisting in correcting deficiencies and escalating non-compliance issues to the ISRMC.
- Initiating third-party assessments to evaluate control effectiveness.
- Promoting user awareness of security practices.

PNB MetLife Best Practices

PNB MetLife shall endeavor to adopt relevant and applicable privacy best practices from Industry and MetLife (i.e., MetLife Privacy Office) to strengthen the policy if and where required.

F. Privacy Risk Assessment

The PNB MetLife shall conduct ongoing privacy risk assessments to identify and evaluate internal and external risks that may result in non-compliance with applicable privacy laws, regulations, and this Policy. These assessments shall be conducted in alignment with the PNB MetLife's Risk Management Framework.

- **Scope of Assessment**

Privacy risk assessments shall, at a minimum, consider the following factors:

- Regulatory Changes: Emerging or revised privacy laws, regulations, and enforcement trends

- Information Security Threats: Including cybersecurity vulnerabilities
- Business Size and Complexity
- Data Governance Practices: Including data lifecycle management and retention
- Third-Party Involvement: Use of external parties for processing Personally Identifiable Information (PII)
- Sensitive Personal Information: Nature and extent of collection and use
- Marketing Practices: Including data usage for profiling or targeted outreach
- Cross-Border Data Transfers: Whether data is transferred or accessed across country borders

➢ **Roles and Responsibilities for PRA**

The Ethics and Compliance team, under the Non-Financial Risk (NFR) program, shall be responsible for conducting privacy risk assessments in accordance with the Risk Management Framework.

Each assessment shall include:

- Inherent Risk Evaluation: Assessment of the nature and magnitude of risk prior to the application of controls
- Control Environment Effectiveness: Review of existing controls and their operational effectiveness
- Testing Results: Consideration of outcomes from prior NFR or Internal Audit testing, where applicable

➢ **Findings from privacy risk assessments shall be used to:**

- Inform risk mitigation strategies
- Enhance privacy governance and control frameworks
- Drive remediation of identified gaps or deficiencies
- Support continuous improvement of processes and practices
- Guide updates to relevant policies, procedures, and training programs
- Strengthen compliance monitoring and reporting mechanisms

▫ **Metrics, Monitoring & Testing**

The NFR team will conduct ongoing oversight, monitoring, and testing in compliance with PNB MetLife's NFR Management Policy/Standard. These oversight activities are the basis for the above-described risk assessments and must be maintained in the appropriate risk management system.

The NFR team, with support from business management, will submit a Quarterly Metrics Report to the MetLife International Compliance Central team. Non -Financial Risk and the Privacy Office analyze relevant privacy metrics, as defined by the Privacy Office, to: (i) identify potential weaknesses in controls; (ii) identify trends and emerging risks; (iii) conduct an overall risk assessment of each operation; and (iv) develop strategies for corrective action in collaboration with business management.

▫ **Information Security**

The Chief Information Security Officer (CISO) and Head of Information Technology are responsible for the implementation and oversight of IT security policies and standards designed to protect data (including personal information) contained in PNB MetLife's applications and databases from unauthorized access, use, alteration, or destruction. They shall meet periodically with the PCG members to review the

effectiveness of the PNB MetLife's administrative and technical data security controls across the enterprise, as assessed by the Information Security team.

G. Internal Audit

Internal Audit shall be conducted periodically, based on risk, and conduct audits to assess implementation of this Policy and compliance with applicable privacy laws/regulations. These audits will include an assessment of the effectiveness and quality of PNB MetLife's procedures, documentation, internal controls, training procedures, Compliance testing, and any corrective actions taken in response to prior audits and examinations by regulators. A written report summarizing the results of the audit and any suggested corrective actions will, at a minimum, be provided to the DPO (as and when applicable), CISO, Head of IT, Chief Risk Officer, the Legal Function, and appropriate senior business management.

H. Policy Review

PMLI Privacy policy will be reviewed and updated (if required) at least annually by the Privacy & Information Security Team.

I. RACI Matrix

Responsible	Accountable	Consulted	Informed
Business Management, Privacy Compliance Group (PCG), Chief Information Security Officer (CISO)	Data Protection Officer (as and when made applicable), Chief Risk Officer, Non-Financial Risk Team including Privacy Team	Legal Department	Board of Directors, All Employees

Key Definitions

Term	Definition
Individuals or Data Subjects	Any natural person about whom personal data is being collected or otherwise processed.
Data Transfer	Any physical, electronic, or other disclosure or dissemination of personal data to another (internal or external) party. Providing access to personal data also amounts to a data transfer.
Personal Data	Any information (alone or in combination with other information) relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly in particular by reference to an identifier, such as a name, an identification number, account number, location data, IP address, internet activity or browsing history, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person. Examples of personal data that by itself can identify the data subject (non-exhaustive list) could be, name, alias, date of birth, home address, telephone numbers and email addresses, an individual's CV or an employee's talent profile, national identification numbers, or identification number which refer to a specific individual such as policy or account number, claim number, credit or debit card number, electronic device ID and bank details.
Processing	Any operation that is performed upon personal data, whether by automated means, including but not limited to collection, recording, accessing, structuring, use, storage, alteration, retrieval, consultation (reading), disclosure, transfer, transmission, anonymization, pseudonymization, dissemination or otherwise making it available, deletion and destruction.
Sensitive Personal Data	A sub-category of personal data which by nature is sensitive as it relates to the data subject's most intimate and if misused could have a significant impact on the data subject. Many data protection and privacy laws impose restrictions or prohibitions, stipulate conditions or require additional safeguards for the processing of sensitive personal data. Some examples (non-exhaustive list) include health or medical conditions, disabilities, addictions, genetic code, biometric data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, offences or criminal convictions and administrative sanctions, credit and debit card details, credit history, national ID, taxpayer identification number, passport number, driver's license number and other unique identification numbers issued by government.

[End of Document]