Privacy Policy

Ver. 2.1 | DPMC, Aug 17, 2024

Table of Contents

Document Control

Current version	Ver. 2.1
Prepared by / date	Consultant, Aug 07, 2024
Reviewed by / date	Data Protection Officer, Aug 16, 2024
Approved by / date	DPMC, Aug 17, 2024
Document Status	Active

Introduction

Bhutan Insurance Limited respects your privacy and is committed to protecting your personal data. This Privacy Policy describes how your personal data is protected when you use and/or access our website, product and services.

This Privacy Policy applies to all information we collect, use, process, store, share and dispose your personally identifiable information from:

a. www.bil.bt
b. Products namely LMS [Loan Management System], Insurance System, PPF/GF System, BIL ERP System
c. Providing of Loans, General Insurance, PPF/ GF Services and Claims Support Services

This is the most current and stable version of the policy, in case, to access the archived versions of privacy policy, the same can be done at ***Not Applicable as being the first version of the policy***

We welcome any feedbacks, suggestions or any complaints, matters and concerns you have, can be reported and contacted at

Title: Bhutan Insurance Limited,
Address: Thimphu Head Office
Post Box 779, Chorten Lam, Thimphu, Bhutan.
Contact: #00975-2-339892/93/94
Email: DPO@bil.bt

While we may come across the personally identifiable information to render our products, services or even while serving the employment related requirements, we classify ourselves as under:

Data Controller	**Conditions** Where Bhutan Insurance Limited is a **Data Controller** • For Employees: Employer-Employee relationship • For Customer: Subscription of Bhutan Insurance Limited insurance, credit and PF/GF realted products and services

	Our responsibilities • Determine and document the purpose and how PII will be processed • Prior consent will be obtained, and relevant records retained • Processes for lawful basis • Stores for defined period and dispose upon data retention life expiry • Transfer only in-cases where it is legally mandated or upon data subject's consent using adequate and appropriate secure methods • Will maintain a record of any data breaches
Data Processor	• **NIL**

Terms, definitions, and abbreviations

Term / Abbreviation	Definition
1. LMS	Loan Management System
2. PPF	Private Provident Fund
3. GF	Gratuity Fund
4. ERP	Enterprise Resource Planning
5. DPO	Data Protection Officer
6. BIT	Business Income Tax
7. CIT	Corporate Income Tax
8. PII	Personally Identifiable Information
9. DPIA	Data Privacy Impact Assessment
10. MOIC	Ministry of Information and Communication
11. DITT	Department of Information Technology & Telecom
12. RMA	Royal Monetary Authority

Purpose of PII collection, use, processing, storing, and sharing

We are the sole owners of the information collected where we act as a Data Controller. We only have access to/collect information that you voluntarily give us via email or other direct contact from you. We will not sell or rent this information to anyone.

We will use your information to respond to you, regarding the reason you contacted us. We will not share your information with any third party outside of our organization, other than as necessary to fulfil your request, e.g., to ship an order or similar one.

Unless you ask us not to, we may contact you via email in the future to tell you about specials, new products or services, or changes to this privacy policy.

Privacy protection statement and commitment

This statement informs you of the types of personal data we collect when you visit our websites and how we process them. With this privacy statement we also fulfil our duty to inform you pursuant under the required privacy protection law

Bhutan Insurance Limited is committed to your privacy. The information we have about our customers and users is protected and secure and we work diligently to ensure that preferences regarding the use of your information are honoured.

This Privacy Policy explains the types of personal information we collect and how we use, store, protect and disclose that information.

We build privacy that works for everyone. Protecting our users' privacy and security is a responsibility that comes with creating products and services that are made available for all. We look to these principles to guide our products, our processes, our people in keeping our users' data private, safe, secure and are committed to continually improve the level of protection it requires

Privacy principles and how we practise it

These are the set of shared values governing the privacy protection of personally identifiable information (PII) when processed in information and communication technology systems. PII principals for PII processing as controllers and/or processors, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed. How we practise the Privacy Principles are listed here:

Privacy Principle	Objective of the Privacy Principle	How we practise it
1. Consent / Choice	Permission granted to use personally identifiable information for lawful purposes	1. For Investment Department they have content declaration to disclose the information which is stated at the bottom of loan application form. 2. Similarly, insurance department also do the consent declaration which was mentioned at the bottom of Insurance Proposal Form. 3. For claims and finance department, they don't declare any consent choice since they are not directly in contact with the customers.
2. Limited Collection / Legitimate Purpose / Purpose Specification	States the purpose for which personal data are collected The subsequent use limited to the fulfilment of those purposes, or such others as are not incompatible with purposes defined	Type: **Customers**: Purpose of PII data maintained under: 1. PII Inventory Register 2. DPIA Register 3. Customer onboarding applications Type: **Employees:** 1. BIL ERP 2. Employee Files maintianed by HR
3. Disclosure Limitation / Transfer to Third Parties / Trans-Border Concerns	Specifies the personally identifiable information (PII) can only be disclosed for the purposes identified under notice and consent It may also mean that PII data be disclosed outside of jurisdictional boundaries as per the legal and contractual requirement only	1. BIL does not disclose the PII data of the customers and employees with any of the: • Third Parties • Transborder sharing 2. BIL may be required to shares PII data with: • Regulators (RMA, etc.) • Governments (MOIC, DITT, etc.)

Privacy Principle	Objective of the Privacy Principle	How we practise it
		• Law Enforcement Agencies (such as court, etc.)

4. Access Limitations	Ensures that access to information is limited only to individuals who specifically require access
	It specifies appropriate safeguards to prevent unauthorized access to personally identifiable information
		Logical as well as Physical access enabled are as under:
		• **Write / Full Access:**
		  • Developers
		  • Networks Administrators
		  • Head IT
		  • Operations
		  • Accounts & Finance
		  • Asst. Manager (IT)
		• **Read / View Access:**
		  • HR & Admin Officer
		  • Operations
		  • Accounts & Finance
		  • Internal and External Auditors
		  • Regulators & Governments
		  • Law Enforcement Agency

5. Security	Safeguards (administrative, technical, operational, and physical controls) to protect personally identifiable information	**Administrative Control:** • Information Security Policies • Data Privacy Policies • Information Security • Risk Management Policy • Data Breach Management and Handling Policy • Data Retention Policy • Data Privacy Impact Assessment • Segregation of Duties

Privacy Principle	Objective of the Privacy Principle	How we practise it
		Technical Control: • Logical access controls • Baseline Hardening • Audit Trail and Audit Logs enabled • Entry/Exit Register • Data Encryption / Data Masking **Operational Control:** • Process Operating Procedures • PII Inventory Register • Data Privacy Impact Assessment Register • Business Impact Analysis Register • Information Security Risk Register • User Access Review • Internal Audits *(Operations & Information Systems and Security)* **Physical Control:** • Physical entry / exit controls to sensitive areas • Fire detection and suppression system • CCTV installed • Safe / Lockers / Cabinet with lock and key
6. Accuracy, Completeness and Quality	Specifies organizations responsible for ensuring its accuracy, completeness, and quality	• Annually, PII Inventory register is reviewed
7. Management, Designation of Privacy Officer, Supervisor Re-Authority, Processing	Ensure formally accountability to safeguard personally identifiable information is assigned and under the BIL's control	• Data Protection Officer (DPO) is appointed • Roles, Responsibilities and Tasks are defined for DPO

Privacy Principle	Objective of the Privacy Principle	How we practise it
Authorization, Accountability		
8. Transparency and Openness	Ensure policies are readily available to individuals and be clear on the intended use of an individual's personal information	• BIL acting under the capacity of Data Controller, the purpose of PII Data Collection, Storing, Processing, and Sharing / Disclose is communicated before PII Data is accessed • Data Principles / Data Subjects consent is obtained before PII Data collected / stored / processed, Transferred / Disclosed
9. Proportionality, Use and Retention, Use Limitation	Protect an individual's personally identifiable information by restricting the use of data and ensuring that organization destroy information when it is no longer in use	• Data is retained post completion of the activity as per Data Retention Policy
10. Access and Individual Participation	Ensure that individuals have the right to request information about them	• BIL ensures Data Subject enjoys their PII Data Access Rights, mandatorily

11. Notice, Purpose and Specification	Ensures that organizations provide notice to individuals about the organizations' policies and procedures regarding the collection, use, process, store, retention, dispose, and disclosure of data	• Notice is in form of Purpose which are covered within respective:
		  • Business services subscriptions
		  • Business application

12. Additional Measures for Breach Notification	Ensure that organizations have specific policies and procedures for notifying individuals in the event of a data breach	• Data Breach Management and Handling policies-cum-procedures are defined

Notes:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   a. Unless Data Principal have ***provided the consent lawfully***
   b. In the case of children under the age of **18**, ***consent is provided by the legal guardians or the parents of the minor***

2. Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate administrative, technical, operational and physical safeguards and measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the jurisdiction application to this policy, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Our privacy jurisdiction applies to

The defined privacy policy covers and reflects the privacy requirements and compliance towards following territory:

Entity Name	**Bhutan Insurance Limited, Thimphu - Bhutan**
Regulations	**Data Privacy and Data Protection Guidelines 2022**
PII Collected	**The same are defined within PII Inventory Register**
Purpose of collection	**The same are defined within PII Inventory Register**
How long we hold the information	Country and Regulator Norm: **10 Years**

Your rights and the obligations

We respect privacy and do same to your exclusive rights under the privacy protection.

You can exercise the following privacy rights all or any one of applicable and requried:

- Right of access - Access your data

- Right to withdraw consent - Withdraw your consent
- Right to object - Object to the processing of your data
- Right to rectification - Correct your data
- Right to erasure - Have your data deleted
- Right to data portability - Transfer your data
- Right to restriction of processing - Restrict processing
- Automated individual decision-making - Be protected from Automated Decision Making
- Right to lodge a complaint - Complain to DPO and DPA

We have defined the process to ease you in accessing your privacy rights and can be found at **Privacy Principals Rights Procedures**

With whom PII is shared / transferred

We do not transfer, share, sell or rent any of your Personally Identifiable Information (PII). However, we may be requried to store PII with appointed third parties in concurrence to this privacy policy.

We require all our third parties and its sub-contractors, if any, to respect the security of your personal data and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with established standards, processes and instructions.

We may be required to share your personal data in case:

Conditions to share	Data Controller	Data Processor
1. Instructed by Privacy Principals	• Hand-over of the PII Data to Privacy Principals upon	• Hand-over of the PII Data to Privacy Principals upon

Conditions to share	Data Controller	Data Processor
	request and as per the business requirements	request and as per the business requirements
2. With our third-party service providers	• Not Applicable	• Not Applicable
3. Routine business process	• Review • Approval • Authorizations • Audits • Compliance	• Inter-department transfer / sharing for business transactions
4. Within entity	• Inter-department transfer / sharing for business transactions	• Inter-department transfer / sharing for business transactions
5. Legal requirement	• Mandate Compliance • Lawful requirements	Not Applicable

What security and privacy protection we applied?

Security and Prevention Controls (SPC) definition: It covers administrative, technical, procedural, and physical safeguards to protect the information in order to control, detect, prevent and correct from un-intended or accidental usages.

Privacy Protection Controls (PPC) definition: These are controls implemented additionally above the SPCs stated, which comprises legal, contractual and any mandatory requirements

As technology evolves, our privacy controls evolve as well, ensuring that privacy is always an individual choice that belongs to the user.

Security and Prevention Controls (SPC)	Privacy Protection Controls (PPC)
• Management control covering policies, procedures, standards, benchmarks and guidelines • Information Security Manager to be In charge handling information security management systems • Authentication and Authorization control • Information classification and identification • Protection from malware • Software updates and patching • System hardening • Network protection and access control • Periodic user awareness, education and training • Cryptography and Encryptions • Activity monitoring • Secure deletion process • Data Protection Arrangement • Infromation security incident handling and reporting procedure • Adequate physical and environmental controls • CCTV Camera for sensitive and confidential areas	• Data Protection Officer to be Incharge of all PII Data realted practices and safeguards • PII inventory register maintenance • Data Principals sufficient privacy notice and consent to be obtained • Documenting the need and purpose of PII Data collection • Articulating Privacy Principles and practicing within every process's *privacy by-design and by- default* • Allowing privacy rights to exercise • Accountability, Audit, and Risk Management • Governance and Privacy Program • Personally identifiable data classification • Data Privacy Impact Assessment • Privacy Requirements for our service providers, consultants and contractors as applicable • Privacy Data Monitoring and Auditing • Periodic privacy awareness, education and training • Data Privacy Breach handling and reporting procedure • Privacy Enhanced System Design and Development • Privacy information retention and periodically destruction • Communication related to privacy requirements

Special Category PII and how we secure

Special Category PII (SCP): currently there are **NIL SCP** applicable to us

In case the SCP if it becomes applicable, then

Special category PII needs more protection considering its sensitivity and confidentiality nature. We determine condition for processing special category data before we begin any processing that may be required under any applicable legal requirements, and ensure that:

a. We document such Special Category PII processing
b. We obtain explicit written consent
c. We state the purpose of collection, use, processing and storing
d. We ensure processing is in accordance with the lawful basis
e. We make all related parties educated and aware on the conditions to process such Special Category PII
f. We assess relevant impacts and required safeguards implemented
g. We check the processing of the special category data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose
h. Where required, we have an appropriate policy document in place
i. We include specific information about our processing of special category data in our privacy information

PII pertaining to minor/children under-age of 18

When a product collects age, and there is an age in your jurisdiction under which parental, guardian or similar person's consent or authorization is required to use the product or services, we will either block users under that age or will ask them to provide consent or authorization from a parent or guardian before they can use it.

We will not knowingly ask infants under that age to provide more data than is required to provide for the product or service.

Communication and Marketing

Where permitted by applicable law and, if required, with your consent, we may send periodic promotional or informational emails to you. You may opt-out of such communications by following the opt-out instructions contained in the e-mail or other communication you may receive. Please note that it may take up to **05 business days** for us to process opt-out requests. If you opt-out of receiving emails about recommendations or other information we think may interest you, we may still send you non-marketing communications about your account or any services you have requested or received from us.

Cookies and other tracking mechanism

For information on the specific tracking mechanisms that we use on our sites, products, services, purposes for which we use such tracking mechanisms, how to disable them, please refer **Cookie Policy**.

Changes to this policy

We regularly review and may make changes to this Policy from time-to-time. To ensure that you are always aware of how we use your personal data we will update the online version of this policy as required from time-to-time to reflect any changes to our use of your personally identifiable information.

We may also make changes to comply with developments in applicable law or regulatory and business requirements. Where it is practicable, we will notify you by other means prior to changes materially affecting you such as by posting a notice on our website or sending you a notification via email. However, we encourage you to review this policy periodically (or at least annually) to be informed of any changes to how we use your personal data.

This Policy was last amended on **Aug 17, 2024, ver. 2.0**

How to contact us

For any questions about this policy or our data protection practices or to exercise any rights you may have in relation to your personal data under applicable law, you can contact us at:

Title: Bhutan Insurance Limited
Address: Thimphu Head Office Post Box 779, Chorten Lam, Thimphu, Bhutan.
Contact: #00975-2-339892/93/94
Email: DOP@bil.bt

Version History

Ver. No.	Year	Particulars of Changes	Prepared By / date	Reviewed By / date	Approved By / date
1.0	2022	Initial draft Privacy Policy format defined.	Consultant Nov 07, 2022	Data Protection Officer Nov 16, 2022	DPMC Nov 17, 2022
2.0	2022	Annual review conducted and NIL changes made	Consultant Aug 07, 2023	DPO Aug 16, 2023	DPMC Aug 17, 2023
2.1	2024	Annual review conducted and NIL changes made	Consultant Aug 07, 2024	DPO Aug 16, 2024	DPMC Aug 17, 2024