Data Privacy Policy

BDBL.PO.037, ver. 1.0 | 02 March 2023 | Data Classification: Internal

Bhutan Development Bank Limited (BDB)

Disclaimer:

Table of Contents

1. Document Control

Ver. No.	Particulars of Changes	Prepared by / Date	Approved by / Date
1.0	Initial Data Privacy Policy defined	Consultant 02.Mar.20	ISSC 02.Mar.20
1.0	Annual review conducted, NIL changes suggested	25.Feb.21	01.Mar.21
1.0	Annual review conducted, NIL changes suggested	25.Feb.22	01.Mar.22
1.0	Annual review conducted, NIL changes suggested	25.Feb.23	01.Mar.23
1.0	Annual review conducted, NIL changes suggested	03.Jan.24	23.Jan.24

2. Introduction

BDB holds personal data about employees, clients, suppliers, and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their work.

In particular, this policy requires employees to ensure that the Information Security Officer (IS Officer) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

This Data Privacy Policy (Policy) outlines how Bhutan Development Bank Limited (BDB) and its other sites and offices collect, process, and use personal information in compliance with applicable laws and regulations.

Personal data is any information concerning a specific or definable natural person

BDB respects the personal data entrusted to us by our clients, vendors, suppliers, contractors, and employees and is committed to ensuring its security through fair and transparent practices.

3. Purpose

It is a disclosure statement and the users are informed about how BDB will collect, store, protect, and utilize personal data that are collected as part of the operations and deliverables

4. Scope

This policy applies to personal/sensitive information either hardcopy or electronic records collected or created by BDB and **tagged as Privacy Information**.

5. Terms, Abbreviations, and Definitions

Sr. No.	Term	Definition
1.	Anonymity	Characteristic of information that does not permit personally identifiable information principal to be identified directly or indirectly
2.	Anonymization	The process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party
3.	Anonymized Data	Data that has been produced as the output of a personally identifiable information anonymization process
4.	Consent	Personally, identifiable information (PII) principal's freely given, specific and informed agreement to the processing of their PII
5.	Identifiability	A condition which results in personally identifiable information (PII) principal being identified, directly or indirectly, based on a given set of PII
6.	Identify	Establish the link between a personally identifiable information (PII) principal and PII or a set of PII
7.	Identity	Set to attributes which make it possible to identify the personally identifiable information principal
8.	Opt-in	Process or type of policy whereby the personally identifiable information (PII) principal is required to take any action to express explicit prior consent for their PII to be processed for a particular
9.	Personally, identifiable information (PII)	Any information that (a) can be used to identify the PII principal to whom such information related (b) Is or might be directly or indirectly linked to a PII principal
10.	PII controller	Privacy stakeholder(s) that determines the purposes and means for processing personally

Sr. No.	Term	Definition
		identifiable information (PII) other than natural persons who use data for personal purposes
11.	PII principal (Data subject)	The natural person to whom the personally identifiable information (PII) related
12.	PII processor	Privacy stakeholder that processes personally identifiable information (PII) on behalf of and under the instructions of a PII controller
13.	Privacy breach	The situation where personally identifiable information is processed in violation of one or more relevant privacy safeguarding requirements Examples of Privacy information protection tools include, but are not limited to, anonymization and pseudonymization tools that eliminate, reduce, mask, or de-identify PII or that prevent unnecessary, unauthorized and/or undesirable processing of PII
14.	Privacy controls	Measures that treat privacy risks by reducing their likelihood or their consequences
15.	Privacy-enhancing technology (PET)	Privacy control, consisting of information and communication technology (ICT) measures, products, or services that protect privacy by eliminating or reducing personally identifiable information (PII) or by preventing unnecessary and/or undesired processing of PII, all without losing the functionality of the ICT system
16.	Privacy policy	Overall intention and direction, rules and commitment, as formally expressed by the personally identifiable information (PII) controller related to the processing of PII in a particular setting
17.	Privacy preferences	Specific choices made by personally identifiable information (PII) principal about how their PII should be processed for a particular purpose
18.	Privacy principles	Set of shared values governing the privacy protection of personally identifiable information (PII) when processing in information and communication technology systems
19.	Privacy risk	Effect of uncertainty on privacy
20.	Privacy risk assessment / Privacy impact assessment	The overall process of risk identification, risk analysis and risk evaluation concerning the processing of personally identifiable information (PII)

Sr. No.	Term	Definition
21.	Privacy safeguarding requirements	Set of requirements an organization has to take into account when processing personally identifiable information (PII) concerning the privacy protection of PII
22.	Privacy stakeholder	Natural or legal person, public authority, agency or any other body that can affect, be affected by or perceive themselves to be affected by a decision or activity related to personally identifiable information (PII) processing
23.	Processing of PII	Operation or set of operations performed upon personally identifiable information (PII) Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.
24.	Pseudonymization	The process applied to personally identifiable information (PII) which replaces identifying information with an alias
25.	Secondary use	Processing of personally identifiable information (PII) in conditions which differ from the initial ones Examples: a new purpose for processing PII, a new recipient of the PII, etc.
26.	Sensitive PII	Category of personally identifiable information (PII), either whose nature is sensitive, such as those that relate to the PII principal's most intimate sphere, or that might have a significant impact on the PII principal
27.	Third-party	Privacy stakeholder other than the personally identifiable information (PII) principal, the PII controller and the PII processor, and the natural persons who are authorized to process the data under the direct authority of the PII controller or the PII processor
28.	Business purposes	The purposes for which personal data may be used: Personnel, administrative, financial, regulatory, and business development purposes. **Business purposes include the following:**

Sr. No.	Term	Definition
		• Compliance with legal, regulatory and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring business policies are adhered to (such as policies covering email and internet use) • Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring, and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration, and assessments • Monitoring staff conduct, disciplinary matters • Marketing our business • Improving services
29.	Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract, and other staff, clients, suppliers, and marketing contacts. Personal data we gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.
30.	Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal or related proceedings—any use of sensitive personal data should be strictly controlled under this policy.

6. Statutory Regulations

This Policy includes the minimum standards for data privacy applicable to BDB. This Policy is primarily derived from the following ISO/IEC 29100 Information technology -- Security techniques -- Privacy framework

Where applicable, Bhutan Development Bank Limited (BDB) seeks to exceed these standards to ensure compliance with stringent laws.

7. Roles and Responsibilities

7.1. Data privacy responsibilities by IS Officer

1. Keeping the board updated about data protection responsibilities, risks, and issues
2. Reviewing all data protection procedures and policies regularly
3. Arranging data protection training and advice for all staff members and those included in this policy
4. Answering questions on data protection from staff, board members and other stakeholders
5. Responding to individuals such as clients and employees who wish to know which data is being held on
6. Checking and approving with third parties that handle the organization's data any contracts or agreement regarding data processing

7.2. Responsibilities of the ICT Administrators

1. Ensure all systems, services, software, and equipment meet acceptable security standards
2. Checking and scanning security hardware and software regularly to ensure it is functioning properly
3. Researching third-party services, such as cloud services the company is considering using to store or process data

7.3. Responsibilities of the Marketing / Business Development

1. Approving data protection statements attached to emails and other marketing copy
2. Addressing data protection queries from clients, target audiences or media outlets
3. Coordinating with the IS Officer to ensure all marketing initiatives adhere to data protection laws and the organization's Data Protection Policy

8. Kinds of Personal Data

BDB has four broad categories of personal data and it is as below:

8.1. Complaint, investigation and legal assistance records

This includes records containing information supplied by data subjects and data users and collected in connection with complaints, investigations, legal assistance, and related activities under the relevant provisions of the Ordinance.

8.2. Personnel records

This includes job applications and BDB's staff personal details, job particulars, details of salary, payments, benefits, leave and training records, group medical and insurance records, mandatory provident schemes participation, performance appraisals, and disciplinary matters, etc.

8.3. Other records

This includes administration and operational files, personal data provided to the BDB from individuals for participating in promotional activities, records relating to education and training activities organized by the BDB, newsletters subscriptions, data relating to consultancy services, compliance check records,

matching procedure applications, records of inspections of personal data systems and inquiries from the public, etc.

8.4. Records collected on webservers

This includes email addresses (whereas they constitute personal data under specific circumstances that the addresses can be used to identify an individual) collected for a subscription.

9. Main Purposes of keeping Personal Data

9.1. Complaint and investigation records

This record is kept to respond to and take follow-up action on complaints, including conciliation between the parties concerned, investigation, if appropriate, and any enforcement or prosecution; **legal assistance records** are kept for the purposes which are directly related to the processing of the legal assistance applications and any subsequent legal proceedings.

9.2. Personnel records of employees

This record is kept for recruitment and human resource management purposes, relating to such matters as employees' appointments, employment benefits, termination, performance appraisal, and discipline, etc.

9.3. Other records

This is kept for various purposes which vary according to the nature of the record, such as administration of office functions and activities, seeking advice on policy or operational matters, organizing and delivering promotional, educational and training activities, acquisition of services, subscription of publications, handling of compliance checks, data matching procedure applications, carrying out of inspections of personal data systems and inquiries from the public, etc.

9.4. Records collected on webservers

This is kept to send letters to subscribers registered through the websites.

10. Information collected when you visit our websites

10.1. Use of cookies

When you browse this website, cookies will be stored in your computer's hard drive. The purpose of using cookies is to facilitate the successful redirection to the correct page upon clicking on the changing banner. We do not collect or store any personal data from you under this circumstance. You have a choice not to accept the cookies, but if you do, certain functionality, i.e. banner redirection, may not be available.

10.2. Statistics on visitors to our websites

When you visit BDB's websites, we will record your visit only as a "hit". The webserver makes a record of your visit that includes your IP addresses (and domain names), the types and configurations of browsers, language settings, geo-locations, operating systems, previous sites visited, and time/duration and the pages visited (webserver access log).

We use the webserver access log to maintain and improve our websites such as to determine the optimal screen resolution, which pages have been most frequently visited etc. We use such data only for website enhancement and optimization purposes.

We do not use and have no intention to use the visitor data to personally identify anyone.

10.3. Outsourcing arrangements

The BDB's internal ICT systems are developed and maintained by in-house staff and a local third-party service provider wherever applicable. The third-party service provider does not have access to personal data stored in the ICT system except when it is carrying out troubleshooting on it at BDB under the supervision of BDB's staff.

10.4. Protection measures

The BDB takes appropriate steps to protect the personal data we hold against loss, unauthorized access, use, modification, or disclosure.

10.5. Retention

BDB maintains and executes retention policies of records containing personal data to ensure personal data is not kept longer than is necessary for the fulfillment of the purpose for which the data is or is to be used. Different retention periods apply to the various kinds of personal data collected and held by the BDB following policies in standing instructions and administration manuals.

11. Privacy by design and default

1. Privacy by design is an approach to projects that promote privacy and data protection compliance from the start.
2. IS Officer will be responsible for conducting **Privacy Impact Assessments** and ensuring that all IT projects commence with a **privacy plan**.
3. When relevant, and when it does not harm the data subject, privacy settings will be set to the most private by default.

12. Scope

1. This policy applies to all people working at the organization.
2. You must be familiar with this policy and comply with its terms.

3. This policy supplements our other policies relating to internet and email use.
4. We may supplement or amend this policy by additional policies and guidelines from time to time.
5. Any new or modified policy will be circulated before being adopted.

13. Who is responsible for this policy

Our IS Officer, has overall responsibility for the day-to-day implementation of this policy.

14. Training

1. All staff will receive training on this policy.
2. New joiners will receive training as part of the induction process.
3. Further / refresher training will be provided at least annually or whenever there is a substantial change in the law or our policy and procedure.
4. Training is provided in-house and will cover:
    4.1. The law relating to data protection
    4.2. Our data protection and related policies and procedures.
5. Attending and completing training is compulsory.

15. Procedures to be followed

15.1. Fair and lawful processing

1. We must process personal data fairly and lawfully under individuals' rights.
2. This generally means that we should not process personal data unless the individual whose details we are processing has provided the consent on it.

The processing of all data must be:

Necessary to deliver our services

1. In our legitimate interests and not unduly prejudice the individual's privacy
2. In most cases, this provision will apply to routine business data processing activities.
3. Our Terms of Business contains a Privacy Notice to clients on data protection.

The notice

1. Sets out the purposes for which the organization hold personal data on customers and employees
2. Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
3. Provides that customers have a right of access to the personal data that we hold about them

16. Privacy Principles

Bhutan Development Bank Limited (BDB) performs the roles of a data controller and data processor during the business.

BDB acting as Data Controller	Determine the purposes and manner in which personal data is processed
BDB acting as Data Processor	Process personal information on behalf of another group company or a third party

17. Choice and Consent

1. Where required by law, Bhutan Development Bank Limited (BDB) obtains consent from individuals to collect, use, retain, or disclose their data.
2. Individuals are given the choice to opt-in or opt-out of this procedure. If applicable, we inform individuals of the consequences for failing to consent or provide their data and the process to alter their consent decisions.
3. Bhutan Development Bank Limited (BDB) verifies that the use of personal data is consistent with the consent obtained.
4. If personal data will be used for a purpose other than that originally disclosed to the individual, we acquire additional consent.

18. Purpose, legitimacy, and specification

1. Bhutan Development Bank Limited (BDB) will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented.
2. All people who are responsible for processing personal data will be aware of the conditions for processing.
3. The conditions for processing will be available to data subjects in the form of a privacy notice.
4. Bhutan Development Bank Limited (BDB) will process personal data in compliance with applicable data protection principles.
5. Bhutan Development Bank Limited (BDB) will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

19. Collection Limitation

Bhutan Development Bank Limited (BDB) collects personal data in a fair, transparent, and lawful manner. As such, the following guidelines adhere to:

1. Collect the minimum personal data required to support a Bhutan Development Bank Limited (BDB) business activity or as mandated by law or service contract.
2. Collect personal data in a fair and non-deceptive manner.
3. Collect personal data directly from the individual, when possible.
4. Where required by law, obtain explicit consent from individuals, before the collection of sensitive personal information (e.g. race, ethnic origin, health details, sexual orientation, etc.); and
5. Verify that personal data collected from third parties is reliable and legally obtained.
6. Furthermore, Bhutan Development Bank Limited (BDB) monitors the involvement of third parties during collection and conducts due diligence to ensure their compliance with this and other required policies.

20. Data minimization

Bhutan Development Bank Limited (BDB) will minimize the data collected that is processed and avoid observability and likability of data collected; Delete and dispose of the data collected whenever the purpose of PII processing has expired

21. Use, Retention, and Disposal

1. All personal data collected by Bhutan Development Bank Limited (BDB) is used expressly for legitimate business activities and purposes consented to by the individual.

2. Bhutan Development Bank Limited (BDB) only uses personal data in strict adherence to contractual, regulatory, and applicable laws.

21.1. Retention

Bhutan Development Bank Limited (BDB) does not retain personal data any longer than is necessary. The retention period for personal data is determined by:

1. The purpose of the data collected,
2. The fulfillment of that purpose, and
3. Mandatory adherence to local and national regulations.

As part of our retention practices, Bhutan Development Bank Limited (BDB) documents, and tracks:

1. Retention periods, as mandated by any contractual and/or regulatory requirements.
2. The mode of storage, archival and back up of personal data collected; and
3. Approval-based disposal procedures (e.g. destruction and redaction) and exceptions to these procedures.

21.2. Disposal, Destruction, and Redaction of Personal Data

Bhutan Development Bank Limited (BDB)'s **Data Retention and Disposal Policy** require managerial approval for the disposal, destruction, and deletion of any personal data. Our disposal, destruction, and redaction procedures prevent the recovery, theft, misuse, or unauthorized access of personal data. For more information regarding this process, please refer to the Bhutan Development Bank Limited (BDB) Data Retention and Disposal Policy.

22. Disclosure to Third Parties

Bhutan Development Bank Limited (BDB) may disclose personal data to third parties as a part of normal business operations. Such third parties must enter into a written contract containing appropriate privacy clauses. Third parties are mandated to handle all personal data under the following:

1. Third parties must ensure equal care and adequate levels of protection; and
2. Appropriate security measures must be implemented to safeguard the personal data; and
3. The personal data must only be processed under Bhutan Development Bank Limited (BDB)'s instructions.

Bhutan Development Bank Limited (BDB) will ensure that international transfers of personal data are afforded with an adequate level of protection, as required by law.

23. Accuracy and Quality

Bhutan Development Bank Limited (BDB) informs individuals that they have a responsibility to provide accurate, complete, and relevant information to maintain the quality and integrity of all personal data. Individuals may contact our designated personnel for any updates or corrections. Individuals may verify and challenge the accuracy and completeness of their data and have it amended or deleted if appropriate. Additionally, Bhutan Development Bank Limited (BDB) has a system in place to record the date, edits, validation, and verification of all personal data collected, maintained and updated.

24. Openness, Transparency, and Notice

Bhutan Development Bank Limited (BDB) informs individuals of the purpose for which it collects, processes, stores, and/or discloses their information through a notice. At the bare minimum, the notice includes:

1. The type of personal data collected.
2. The purpose for which it is collected.
3. The legal requirement to collect this personal data (if applicable).
4. How personal data will be used or processed.
5. How individuals can access their data and amend it for accuracy.
6. An explanation of third-party involvement in processing personal data (if applicable).
7. The consequences, if any, for not providing the requested personal data; and.
8. An option for individuals to indicate a preferred means of contact.

The notice is drafted in simple and clear language in a format that is consistent across the organization.

The document also contains the geographic area, office locations, jurisdiction, and name of the Bhutan Development Bank Limited (BDB) entity that issues the notice.

25. Individual participation and access

1. All individuals are given access to review, update, or correct their data. The mode of access to this information is communicated to the individual within an appropriate timeframe.
2. Where required by law, Bhutan Development Bank Limited (BDB) will respond to requests from individuals to provide them with information relating to the personal data, that Bhutan Development Bank Limited (BDB) holds about them.
3. Furthermore, Bhutan Development Bank Limited (BDB) authenticates individuals before granting access to personal data. Access to personal data may be denied if an unreasonable request is made, subject to laws.

If access is denied, Bhutan Development Bank Limited (BDB) provides the reason and a point of contact for further inquiry to the individual.

25.1. Protection of Personal Data in the possession of third-parties

1. Bhutan Development Bank Limited (BDB) conducts appropriate due diligence checks before and during the selection of third parties who process personal data on behalf of Bhutan Development Bank Limited (BDB).

2. Bhutan Development Bank Limited (BDB) requires third parties to strictly adhere to contractual terms and guidelines on data protection to the extent such third parties have access to or are otherwise processing personal data on behalf of Bhutan Development Bank Limited (BDB). Furthermore, Bhutan Development Bank Limited (BDB) retains the audit rights to monitor and supervise all Bhutan Development Bank Limited (BDB) provided personal data that is processed or handled during the performance of services by a third party contractor.

3. Finally, Bhutan Development Bank Limited (BDB) maintains a well-defined mitigation and remediation plan if any harm may result due to third party misusing or improperly processing such Bhutan Development Bank Limited (BDB) provided personal data in violation of contractual and statutory obligations.

26. Security

1. Bhutan Development Bank Limited (BDB) has implemented physical, administrative, and technical security measures across the organization which is designed to prevent data loss, unauthorized access to personal data and misuse, disclosure, alteration, damage, or destruction of personal data.

2. Bhutan Development Bank Limited (BDB) fully understands that the personal data collected from individuals is under the organization's guardianship. Therefore, we train our employees on the privacy policy as well as information security procedures regarding the appropriate access, use, and disclosure of personal data. Bhutan Development Bank Limited (BDB) also conducts periodic risk assessments on our processes, information systems, and third parties, including audits of third party facilities and information systems.

3. Bhutan Development Bank Limited (BDB) has in place an incident response plan with trained personnel to respond to, investigate, and mitigate the impact of any incident. Bhutan Development Bank Limited (BDB) also maintains adequate plans for business continuity management, as well as disaster recovery processes for testing databases, servers, information systems, and processes that handle personal data.

27. Compliance and Reporting

Bhutan Development Bank Limited (BDB) is committed to monitoring and enforcing compliance with this Policy and with applicable privacy laws, regulations, and obligations. Documented procedures are defined for:

1. Addressing and resolving any data privacy grievance;
2. Implementing a remediation process for any data privacy breach; and
3. Identifying a third-party arbitrator for dispute resolution, if necessary.

Also, employees, customers, and third parties can submit questions, concerns, or complaints about Bhutan Development Bank Limited (BDB)'s privacy practices to our IS Officer.

Any potential or actual violation of this Policy is immediately reported to our Chief Compliance Officer.

27.1. Compliance Review

Bhutan Development Bank Limited (BDB) conducts regular audits of our compliance with applicable privacy policies, procedures, laws, regulations, contracts, and standards.

During the compliance review, the following is considered:

1. Document the processes for the resolution of issues and vulnerabilities, as well as corrective action plans;
2. Record the results of compliance reviews and regularly submit material findings to the **ISSC** and Board of the company; and
3. Follow up on recommendations for improvement/remediation plans based on the results of the compliance review.
4. Accesses granted on PII shall be reviewed at least Quarterly.

All Bhutan Development Bank Limited (BDB) directors, officers, employees, agents, and contractors are expected to fully comply with this Policy.

27.2. Consequences of failing to comply

1. Violations of this Policy are investigated, and failure to comply with this Policy may result in disciplinary action up to and including termination of employment or contract.
2. We take compliance with this policy very seriously.
3. Failure to comply puts both you and the organization at risk.
4. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under disciplinary procedures which may result in dismissal.
5. Advice and opinion form the legal team would be soughed out wherever required.
6. If you have any questions or concerns about anything in this policy, consult with the IS Officer.

28. References

Policy	Standard: ISO/IEC 27001:2023 Annex. A
	Standard: ISO/IEC 29001:2011 Privacy Framework
Procedure	Nil
Guidelines	Nil
Records/Templates	Nil

29. Record Retention and Disposal

Sr. No.	Document Name / No.	Document Type	Retention Period	Storage Location	Disposal Method	Owner
1.	Nil	NA	NA	NA	NA	NA

Note:
Document Type : HC = Hard Copy, SC = Soft Copy
Retention Period : EOL = End of Life, Tenure such as 1 Yr., 2 Yr.
Storage Location : SP = Shared Path, C = Cabinet
Disposal Method : NA = Not Applicable, SH = Shred, DEL = Delete, DG = Degaussing

30. Enforcement and Implementation

Each department/unit is responsible for implementing, reviewing, and monitoring to assure compliance with this policy. The Information Security Officer is responsible for enforcing this policy.

31. Consequences and Sanctions

Non-compliance with this policy/procedure/standard may incur the same types of disciplinary measures and consequences as violations of other policies, including progressive discipline up to and including termination of employment.

Any device that does not meet the minimum-security requirements may be removed from the corporate network, disabled, etc. as appropriate until the device can comply with this policy.

32. Exceptions

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate academic or business needs.

33. Communication and Training

Will this document be publicized through Internal Communications?	**Yes**
Will training needs arise from this document	**Yes**