Classification: Internal

BHARTI AXA LIFE INSURANCE INFORMATION SECURITY

Data Privacy Policy

Version 4.9 – 2024

Contacts for this document

Role	E-Mail	Entity
Chiragali M Peerzada – Assistant Vice president – Risk Control	Chiragali.peerzada@bhartiaxa.com	Bharti AXA Life Insurance

Approval

Person	Position	Status	Date
C L Baradhwaj	SVP, Compliance and Risk Head	Approved	
Rajeev Kumar	Principal Officer	Approved	
Board	Board	Approved	26-July-2017
Board	Board	Approved	07-Mar-2018
Board	Board	Approved	30-Oct-2018
Board	Board	Approved	14-May-2019
Board	Board	Approved	13-May-2020
Board	Board	Approved	21-May-2021
Board	Board	Approved	16-May-2022
Board	Board	Approved	26-July-2024

Document Control

Document Location:	Internal Web Portal
Review Frequency:	This document will be reviewed once Annually
Document Sensitivity	Internal

Revision history

Rev.no	Date of change	Summary of Change	Reviewed by
1.0	09-Feb-2009	Initial version	Ajay Patil
2.1	14-May-2012	Updated in line with GISPS v 2.1	Ajay Patil
2.2	17-June-2014	Updated in line with AISP v 2.0	Sandesh Bagwe
3.0	07-Dec-2016	Annual Review	Nelson Yaragal
4.0	17-July-2017	Reorganized the existing policy as per IRDAI guidelines. Document ID, name and version number updated	Shilpa Jabde
4.1	10-Jan-2018	Review Done. Service provider update in some of the annexes of Board approved Information Security policy.	Shilpa Jabde

4.2	10-Oct-2018	Review Done. No major Changes	Ganesh A. Kshirsagar & Shilpa Jabde
4.3	16-Apr-2019	Minor changes related to GDPO as its not applicable, removed from policy.	Ganesh A. Kshirsagar & Shilpa Jabde
4.4	18-Mar-2020	Policy Reviewed. No Changes	Shilpa Jabde & Ganesh A. Kshirsagar
4.5	22-Mar-2021	Reviewed No Changes	Chiragali Peerzada
4.6	27-JAN-2022	Aligned as per ISO 27001:2013 Standards	Chiragali Peerzada
4.7	09-JAN-2023	Reviewed No Changes	Chiragali Peerzada
4.8	14-July-2023	Updated as per Revised IRDAI Guidelines	Chiragali Peerzada
4.9	26-July-2024	Annual Review – No Changes Done.	Chiragali Peerzada

Contents

1 Purpose

Bharti AXA LI is committed to protecting the privacy of personal information including sensitive personal data or information disclosed to us by customers, partners, and employees. The Data Privacy Policy ('Policy') sets out minimum data protection and privacy requirements of Bharti AXA LI.

2 Objective

The main objective of the Policy is to set out the minimum data protection and privacy requirements in order to:

- Articulate Bharti AXA LI's commitment to protecting data.
- Promote a consistent approach to data privacy and protection across the Group.
- Improve operational efficiency.

3 Scope

The Policy is applicable to

- All employees including contract staff, vendors, and temporary staff.
- Third parties working with us (including intermediaries, agents, and outsourced service providers

4 Responsibility

The CEO is ultimately responsible for ensuring that the Company establishes policies and procedures consistent with this Policy for the collection or use of Personal Data in his business and meeting applicable legal, regulatory, or contractual requirements.

The management of the Data Privacy Framework follows "three lines of defence":

•The Senior and Business Management being the first line of defence are responsible for ensuring Personal Data handling procedures are meeting local requirements and are consistent with this Policy.
•The DPO being the second line of defence supports the Senior and Business Management by means of developing and implementing adequate procedures safeguards and controls to ensure meeting local requirements and consistency with this Policy.
•Internal Audit being the third line of defence provides independent assurance on the effectiveness of the Data Privacy Framework.
•The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the Company or a person handling / processing sensitive personal data on its behalf undertakes significant up gradation of its process and computer resource.

4.1 Division of data privacy roles and responsibilities within Bharti AXA LI:

Bharti AXA LI shall appoint a Data Privacy Officer who is responsible for and has appropriate authority to ensure compliance with this Policy and is an ultimate contact person for any Data Privacy issues. Bharti AXA LI shall ensure that all stated below roles and responsibilities are achieved either solely through its Data Privacy Officer or divide them between its Data privacy Officer and IT Legal, Compliance and/or HR functions.

The Data Privacy Officer empowered to ensure compliance of this policy and related business activities across all functional areas. Executive management of Bharti AXA LI will ensure that adequate funding and other necessary support is available to support the compliance with both its regulatory requirements and additional requirements within group and local privacy policies.

4.2 Roles and responsibilities of Senior and Business Management:

The Senior and Business Management (i.e., Management who decides what, why and how Personal Data is collected and processed) is the first line of defence and responsible for understanding the applicable regulatory requirements and ensuring that the Bharti AXA LI collection, processing, transfer, and retention of Personal Data complies with those regulatory requirements and this Policy.

The senior and Business Management should provide the DPO with the necessary information and means to enable him to support them in ensuring the Bharti AXA LI compliance with this Policy and local requirements. In particular, the senior and Business Management should have regular exchanges with the DPO and keep him informed about relevant organizational or other developments that may have an impact on Data Privacy.

Also, the senior and Business Management should ensure appropriate “tone at the top” communication with respect to awareness of the issues covered by this Policy.

4.3 Roles and responsibilities of Data Privacy Officer:

One of the responsibilities of data privacy officer is to monitor regulations impacting the organization and to adapt the data privacy policy so that compliance with all appropriate regulatory compliance obligations prevails.

The Data Privacy Officer’s main business-oriented data privacy activities are realized with the support of legal, compliance, HR, and information security departments.

- Provides consultative advice to all the areas of the different entities of the Group in privacy matters
- Relation with the relevant regulators.
- Creation, modification, or deletion of the data files in the General Data Protection Register.

- Reporting to the Local Control Authority: Attendance inspections, audit submissions and coordination and information submissions requirements
- Collaboration with the unit(s) responsible to manage the rights of access, rectification and cancellation
- Internal or external confidentiality agreements.
- Review of business activities and vendor contracting to ensure compliance with Local Control Authority and Bharti AXA LI policy requirements.
- Attendance at the Data Protection and Security Committees.

4.4 Roles and responsibilities of data owner maintaining personal data filing system:

- Develop and implement measures aimed at ensuring physical and technical security of the filing systems and confidentiality of their content.
- Develop and implement measures aimed at ensuring the appropriate access and use of confidential information.
- Develop and implement measures aimed at ensuring the appropriate 3rd party sharing and onward transfer of confidential information.
- Ensure communication with current and future data subjects with respect to processing of their personal data (obtaining a relevant data subject's consent, ensuring a data subject's right of access to data, providing a data subject with the information specified by law).

4.5 Obligations of employees and third parties, i.e., insurance intermediaries etc.:

- Develop and implement measures aimed at ensuring data processing by third parties is allowed in only permissible circumstances and that these entities process the data in accordance with applicable local laws
- Obtain necessary reporting from third parties for use with compliance activities and Local Control Authority reporting
- Perform periodic audits of privacy, security, and other necessary compliance activities to ensure overall legal compliance.

5 Definitions

For the purpose of this Act, unless the context otherwise requires the following terms shall have the meaning defined herein:

'Act' means the Information Technology Act, 2000, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and includes subsequent notifications notified thereunder or amendments made thereto.

"Personal Data" or "Personal Information" means any data relating to a Person who can be identified either:

(a) directly from that data; or
(b) from that data together with any other information which either is or likely to be available."

- **Examples of Personal data include:**

Name, pseudonyms, address, telephone number, identity card number, occupation, salary/compensation, health or personal records, birth date, etc.

Personal Information or Personal Data also includes 'Sensitive personal data'.

'Data Subject' or 'Provider of information' is the individual who is the subject of the 'personal data' and can be identified or distinguished from others, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. This includes former and existing data subjects and colleagues, whether individuals, sole traders, or members of a partnership.

"Sensitive personal data or information'— Sensitive personal data or information of a person means such personal information which consists of information relating to; —

- password.
- Financial information such as Bank account or credit card or debit card or other payment instrument details.
- physical, physiological, and mental health condition.
- sexual orientation.
- medical records and history.
- Biometric information.
- any detail relating to the above clauses as provided to body corporate for providing service; and any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise. 'Data Controller' is a person (alone, jointly or with others) who decides how and why personal information is to be processed. In most cases this would be the individual or company that 'owns' the data.

'Data Processor' is any person (but not an employee of the Data Controller) who processes personal data on behalf of the data controller. Data Controllers must ensure the same duty of care is maintained when a third party is processing personal data on their behalf.

The word "Data" and "Information" are used interchangeably in this Policy.

6 Data Privacy Principles

Bharti AXA LI and its employees must adhere to the following 06 (six) principles of data protection:

6.1 Principle-1 Collection of Personal Data:

Personal Data can be obtained only by lawful and fair means and with the knowledge or consent of the Data Subject. Bharti AXA LI or any person on its behalf who/ which is collecting the Personal Data shall obtain a consent of the Data Subject for collection of the information wither in writing, through letter or Fax or e-mail or any other electronic means.

While collecting sensitive personal data or information directly from the Data Subject, Bharti AXA LI or any person collecting such Data on its behalf shall ensure that the Data subject has the knowledge of followings:

a) the fact Bharti AXA LI is collecting the Personal Data.
b) the purpose for which Personal Data is being collected.
c) the intended recipients of Personal Data.

While collecting Personal Data the following should be kept in mind:

a) the information is collected for legitimate purpose only, connected with a function or activity of
Bharti AXA LI or any other defined activity.
b) Where the data is sensitive personal data or information, the same should be collected only where it is considered necessary for Bharti AXA LI to carry out its activity.
c) The Data collected must be relevant and not excessive than the purpose for which it is collected.

6.2 Principle-2 Purpose of Data Collection:

The purpose for which the Personal Data is being collected ("Core Purpose") should be communicated to the Data subject no later than the time of data collection. The subsequent use of the Personal Data should be for the purpose for which the data was collected or any usage which is incidental thereto and required to fulfilment of the purpose.

Further, in case the purpose of data collection is to be extended to any purpose other than core purpose the same must be communicated to the Data subject at the time of collection.

Where the Personal Data collected would include sensitive personal data, the purpose of collection must be necessary.

6.3 Principle-3: Data Quality:

Where the Data Subject has furnished any Data/information to Bharti AXA LI orally, Bharti AXA LI must record such personal data and send to the Data Subject for confirmation and if Data subject points out any correction must carry out the same.

While collecting the Personal Data, Bharti AXA LI shall not annotate the documents of Data Subject nor shall document any information of Data subject which has not been provided by Data Subject.

The Personal Data should be kept up to date by Bharti AXA LI.

Bharti AXA LI shall permit the Data Subjects, as and when requested by them, to review personal data, including the sensitive personal data, provided by them and wherever required/feasible correct the inaccuracy pointed by the Data subject or update/ amend the data.

The Data Subject may, at any time while availing the services or otherwise, be provided an option to withdraw its consent given earlier to Bharti AXA LI. Such withdrawal of the consent shall be sent in writing.

6.4 Principle-4: Data Use:

The Personal Data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the Consent of the Data Subject or if required under the law.

Personal Data can be used only for the purpose for which it was collected and may be shared with a third party engaged by Bharti AXA LI for rendering service related to the Purpose. The Personal

Data must not be sold to anyone without express consent of the Data Subject and other compliances under law. Further, the Personal Data cannot be transferred to a third party without express consent of the Data subject and Data subject must be informed the purpose of transmission, the identity of the third party to such recipient and the rights which the Data subject would have on such transmission. Further, where Bharti AXA LI shares the Personal Data with third party service provider, Bharti AXA LI must ensure that such third party protects the confidentiality of such Personal data before the Personal Data can be shared.

Bharti AXA LI may share the Personal Data, without obtaining prior consent of Data Subject, with Courts, regulatory bodies, and other statutory authorities, if same is required under statute or the disclosure is required under any summon or notice served by such regulatory authorities.
If the Personal data is required to be transferred outside India, the same must be approved by DPO. Further, where Data is transferred to/shared with any entity other than Bharti AXA LI, approval of DPO.
must be obtained and DPO must ensure that following are in place:
1. Applicable laws and regulations relating to transfer/sharing of Personal Data, including the requirement of Data privacy policy are complied with.
2. Ownership of the data is made clear before the transfer/sharing of Data takes place.
3. Any restriction on usage of Data is clearly noted and duly acknowledged by the recipient.

Where the data sharing/ transfer with an entity is routine in nature one-time approval as above would be sufficient unless the Data element to be shared is amended substantially.

Further, DPO must keep records where Personal Data is held /processed outside India and advise if any additional foreign laws/regulations are required to be complied with.

6.5 Principle-5: Data Security:

Personal Data should be protected by reasonable security and safeguarded against risks such as loss or unauthorized access, destruction, use, modification, or disclosure thereof.

Personal Data must be kept secure and the Persons who are not authorized should not have access to or be able to disclose the information. Personal Data must not be retained for any longer than necessary (for the purposes for which it was obtained) and in line with Data Retention Policy of the Company.

6.6 Principle-6: Rights of Data Subject:

Data Subjects have the right to access and correct their Personal Data, and such requests should be acted on and complied with in a timely and reasonable manner (unless there are lawful reasons for denying the request).

Data Subjects can request:
- a copy of the Personal Data relating to them, including information relating to the source of the data.
- a list of the recipients (or categories of recipients) to which their Personal Data is transferred.
- information about the purpose of recording their Personal Data.
- to rectify their Personal Data when it is inaccurate.
- to request deletion of their Personal Data (only if legally possible); and
- to obtain any other information which would be required under local law.

Bharti AXA LI must respond, to the extent feasible, promptly to all such requests from Data Subjects

7 Policy

- While processing the data from different sources, Bharti AXA LI shall follow principles included in the data privacy policy with regard to local regulation.
- Processing of Sensitive personal data is possible only with explicit consent of the data subject to the processing, except where the local laws prohibits its´ processing and it may not be lifted by the data subject's giving his consent, or if it is allowed by local law.
- Appropriate security measures should be put in place to ensure protection of the Personal Data in line with the security policy.
- Used applications for Personal Data processing have to be documented in the register of processing.
- Applications should not be implemented before all technical and legal issues including data processing agreements – if necessary - are executed /prepared.
- Bharti AXA LI shall acquaint all its' users with the principles set out in the Data Privacy Policy.

7.1 Rights of Data Subjects or Information Providers

Data subjects or Information Providers are entitled.

- To be informed, if personal data are recorded for the first time by the data controller for own purposes without the data subject's knowledge, unless the information is not necessary because of legal exceptions.
- To request information about recorded data relating to them, including information relating to the source of the data,
- To request the recipients or categories of recipients to which the data are transferred.
- The purpose of recording the data,
- To rectify data when they are inaccurate.
- Data Privacy Law - A full-fledged Indian data privacy law is expected any time. It will be mandatory to protect data privacy as per this law.

7.2 Personal Data Security Measures

The processing of personal data requires the implementation of an effective system of organizational and technical measures for

- Preventing unauthorized persons from gaining access to data processing systems for processing or using Personal data (access control),
- Ensuring that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control, need to know principle),

- Ensuring that personal data cannot be read, copied, altered, or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- Ensuring that it is possible after the fact to check and to ascertain whether personal data have been entered into, altered, or removed from data processing systems and if so, by whom (input control),
- Ensuring that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- Ensuring that personal data are protected against accidental destruction or loss (availability control),
- Ensuring that data collected for different purposes can be processed separately.
- Data Leakage Prevention (DLP)
  - Data classification standards including data privacy requirements.
  - Liaison with business for understanding business processes and data classification.

The level of the measures for data protection depends on the sensibility of the processing data. Data are classified in the Bharti AXA LI's Information Asset classification policy.

7.3 Data Privacy

Personally, Identifiable Information (PII) is information about a person that contains some unique identifier, including but not limited to name, email, contact details or unique identification number, from which the identity of the person can be determined.
PII may be further bifurcated into –
1. Sensitive Personal Information
2. Other Personal Information Any incident of data privacy violation must be reported immediately to the concerned authority so that the exposure can be contained. Refer to Incident and Problem Management Policy

7.4 Awareness Measures

Persons incorporated in data processing shall not collect, process, or use personal data without authorization (confidentiality). Such persons have to be committed to maintain confidentiality when taking up their duties. The obligation of confidentiality shall continue after their employment ends.

Each data controller has to take appropriate measures to familiarize persons incorporated in the processing of personal data with the recent legal provisions and special requirements of data protection.

Bharti AXA LI must ensure that employees, cooperative persons, contractors who work in Bharti AXA or any other relevant Third Parties are properly informed and trained when involved in the processing of Personal Data with regard to the principles contained in this Policy and any other relevant Data Privacy laws and regulations, rules, and procedures.

The employees of Bharti AXA LI must be provided training on the Data Privacy policy as and when required so as to keep them up to date. The employees must complete the training within the timeframe provided.

7.5 Data Transfer

Data transfer means communication of data to third parties.

Principles:

- Personal data may not be transmitted to third parties without the consent of the data subject.
- Consent may be given in any form allowed in the local legislation.
- Consent must specifically, regarding point 9, refer to the purpose of the transmission, the content of the data to be transmitted and the identity of the recipient. If the data concerns medical documents or sensitive data, then consent must always be given in writing.

Consent of the person concerned is not required:

- When the transfer is authorized by a law.
- When the data have been collected from publicly accessible sources.
- When the communication to be affected is destined for the Ombudsman, the Office of Public Prosecutor, judges, or courts.
- When the transfer of personal data on health is necessary for resolving an emergency which requires access to a file or for conducting epidemiological studies within the meaning of central or regional government health legislation.
- Any other reason established in the local law.

Bharti AXA LI or any person on its behalf may transfer sensitive personal data or information including any information, to any other organization or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the organization as provided for under the IT Rules 2011. The transfer may be allowed only if it is necessary for the performance of the lawful contract between Bharti AXA LI or any person on its behalf and provider of information or where such person has consented to data transfer.

7.6 Third Parties

7.6.1 Providers ofservices

Access to data by a third party shall not be considered communication of data when such access is necessary for the provision of a service to the data controller. Consequently, consent of the data subject is not required when the transmission takes place in accordance with an outsourcing contract with a third party.

7.6.2 Rules for engaging suppliers and use of clouds

Processing on behalf of third parties shall be regulated in a contract which must be in writing or in any other form which allows its performance and content to be assessed, it being expressly laid down that the processor shall process the data only in accordance with the instructions of the controller, shall not apply or use them for a purpose other than that set out in the said contract, and shall not communicate them to other persons even for their preservation.

The contract shall also include confidentiality requirements and set out the security measures referred in regulations.

If the processor uses the data for another purpose, communicates them or uses them in a way not in accordance with the terms of the contract, he shall also be considered as the controller and shall be personally responsible for the infringements committed by him.

The data processor may not subcontract to a third party any processing commissioned to him by the data controller, unless he has received authorization to do so. In that case, the contracting shall always be done in the name and on behalf of the data controller

7.7 Data Retention

Personal data shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which they were obtained or recorded.

Personal data shall be erased when they have ceased to be necessary for the purpose for which they were obtained or recorded.

Previous erase, the personal data shall be stored in a way which permits the right of access to be exercised.

Data may be stored for the duration of any kind of liability arising from legal relations or obligations or the execution of a contract or the application of pre-contractual measures requested by the data subject.

On a regular basis, the procedure for data retention shall be determined by local legislation and a retention schedule must be drawn up.

On the expiry of such liability as stated above, data may only be stored following their dissociation.