BHARTI AXA Life Insurance Company Limited

Data Privacy Policy

Ver.2.0 dated 08 October 2014

A. Data Privacy Policy Description

Bharti AXA Life Insurance is committed to protecting the privacy of personal information including sensitive personal data or information disclosed by us, or to us by customers, distributors, third party service providers and employees. The Data Privacy Policy ('Policy') sets out minimum data protection and privacy requirements of Bharti AXA Life Insurance.

B. Scope of Data Privacy Policy

The Policy is applicable to:

- All employees including contract staff and temporary
- Third parties working with us (including intermediaries, agents and outsourced service providers)
    - Third parties where personal data exchange is not involved are outside the scope of this Policy
- The Directors of the Company

C. Definitions

'Act' means the Information Technology Act, 2000 and includes subsequent amendments to the Act and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011and any other rules/regulations as notified from time to time.

'Personal Information or Data' means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. Examples include: name, address, telephone number, birth date, etc. Personal Information or Data' also includes 'Sensitive personal data or information'.

'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, 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 or sexual life
- medical records and history;
- Biometric information;
- any detail relating to the above clauses as provided to body corporate for providing service; and
- Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Memberships in trade unions
- Criminal record
- Personality profile
- Data representing a behaviour might also be sensitive
- any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

However, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force may not be regarded as sensitive personal data or information.

'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.

'Data transfer' means communication of data to third parties.

D. Data Privacy Principles

Bharti AXA Life and its employees must adhere to the following 6 principles of personal data protection:

1. **Limits apply to the collection of Personal Data. Personal Data can only be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the Data Subject.**

   Bharti AXA Life or any person on its behalf shall obtain consent in writing through letter or Fax or e-mail from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information. Prior to the collection of information including sensitive personal data or information an option to the provider of the information to not to provide the data or information sought to be collected is to be provided.

   Bharti AXA Life or any person on its behalf shall not collect sensitive personal data or information unless —
   (a) the information is collected for a lawful purpose connected with a function or activity of Bharti AXA Life or any person on its behalf; and
   (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

   While collecting sensitive personal data or information directly from the person concerned, Bharti AXA Life or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of:
   (a) the fact that the information is being collected;
   (b) the purpose for which the information is being collected;

(c) the intended recipients of the information; and
(d) the name and address of —
    (i) the agency that is collecting the information; and
    (ii) the agency that will retain the information.

Bharti AXA Life or any person on its behalf shall permit the providers of information, as and when requested by them, to review sensitive personal information or personal data they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible.

The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to Bharti AXA Life. Such withdrawal of the consent shall be sent in writing.

2. The purposes for which Personal Data are collected should be specified not later than at the time of data collection. The subsequent use of Personal Data collected should be limited to the fulfillment of those purposes for which it has been collected.

a. At the time of collecting Personal Data or sensitive personal data from a Data Subject, the Data Subject must be clearly informed about the core purpose of the data collection (e.g. to underwrite an insurance policy), and whether or not that core purpose may be extended to other purposes (e.g. marketing).
b. Personal Data including sensitive personal data must be collected only for specified, explicit and legitimate purpose(s).

3. Personal Data collected should be relevant to the purposes for which it is to be used and (to extent necessary for those purposes) should be accurate, complete and kept up-to-date.

Personal Data including sensitive personal data collected must be relevant and not excessive in relation to its intended purposes.

The Data Subject must be given an opportunity to review the data and if necessary, correct it.

4. Sensitive Data should not be disclosed, made available or otherwise used for purposes other than those specified, Sensitive personal data or information can be shared only with the consent of the Data Subject or if required by law.

Disclosure of Information
Disclosure of sensitive personal data or information by Bharti AXA Life to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the Bharti AXA Life and provider of information, or where the disclosure is necessary for compliance of a legal obligation.

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and

punishment of offences. The Government agency shall send a request in writing to Bharti AXA Life to share the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

Bharti AXA Life or any person on its behalf shall not publish the sensitive personal data or information in public domain.

The third party receiving the sensitive personal data or information from the Company or any person on its behalf shall not disclose it further.

5. **Personal Data should be protected by reasonable security safeguards against risks such as loss or unauthorised access, destruction, use, modification or disclosure of data.**

   Personal Data including sensitive personal data must be kept secure. Persons that are not authorised should not have access to or be able to disclose the information. Sensitive Personal Data must not be retained for any longer than necessary (for the purposes for which it was obtained). Please refer to Bharti AXA Life Data Retention Policy for details on how long sensitive Personal Data is allowed to be retained.

6. **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

Bharti AXA Life must respond promptly to all such requests from Data Subjects.

E. Implementation – Application

While processing the data from different sources, Bharti AXA Life Insurance shall follow principles included in the data privacy policy with regard to local regulation.

Appropriate security measures should be put in place to ensure protection of the Personal Data in line with the Bharti AXA Life Information security policy and Reasonable Security Practices and Procedures prescribed under Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

Bharti AXA Life shall acquaint all its' users with the principles set out in the Data Privacy Policy.

F. Organisational framework

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 and meeting applicable legal, regulatory or contractual requirements.

The management of the Data Privacy Framework follows AXA's model of the "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 Data Privacy Officer being the second line of defence supports the Senior and Business Management in 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 upgradation of its process and computer resource.

o Division of data privacy roles and responsibilities within Bharti AXA Life Insurance

Bharti AXA Life shall appoint a Data Privacy Officer who is responsible for and has appropriate authority to ensure compliance with this Policy and is the initial contact person for any Data Privacy issues. Bharti AXA Life shall ensure that all stated 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 Compliance Head will be the data privacy officer. The Data Privacy Officer will be empowered to ensure compliance of this policy and related business activities across all functional areas. Executive management of Bharti AXA Life 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 data privacy policy.

o 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 Life 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 Life's compliance with this Policy and local requirements. In particular, the senior and Business

Management should have regular exchanges with the DPO and keep him/her informed about relevant organisational 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.
Bharti AXA Life must ensure that employees, cooperative persons, contractors who work in the Company or any other relevant Third Parties are properly informed 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.

- **Roles and responsibilities of Data Privacy Officer**

One of the responsibilities of data privacy officer is to monitor regulations impacting the organisation 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 realised with the support of legal, compliance, HR and information security departments.

Key Responsibilities:

Policy, Procedures, and Compliance

Oversee compliance with the Information Technology Act, 2000, Information Technology Act, 2008, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, Bharti AXA Life Data Privacy Policy and any other relevant requirements including.

- Implementing and maintaining systems and controls to meet the local legal requirements
- Develop Bharti AXA Life's Data Privacy policy, ensure the incorporation of approved exemptions, if any, and keep the Data Privacy Policy up-to-date.
- Monitor local regulations and adapt local Data Privacy Policy to oversee compliance with applicable laws.
- Develop and execute an appropriate regulatory monitoring plan and reporting.
- Coordination and management of responses to incidents involving Personal Data (e.g. unauthorised access or disclosure);
- Oversee that the business (applications and process) is compliant with the Data Privacy requirements and local Data Privacy legislation.
- The DPO must keep a formal record of any Personal Data that are routinely held or processed outside the country of origin and must ascertain if there are any additional laws or regulations that need to be complied with as a result.
- Ensuring on a regular basis that data processing applications and processes are compliant with local Data Privacy legislation and Policy requirements.
- Reviewing and monitoring business activities and vendor contracting to oversee compliance with local Data Privacy legislation and the Policy requirements;

- Ensure inclusion in project and process sign-off procedures and providing Data Privacy sign-off when satisfied that each project or process is compliant with the Policy and applicable local requirements.

Governance

- Manage and coordinate relationships in order to facilitate completion of Data Privacy related goals and requirements and communication of Data Privacy related matters. Specific tasks include, but are not limited to:
- Manage the relationship with the Group Data Privacy Officer (GDPO), the Regional Data Privacy Officer, and other Data Privacy Officers.
- Coordination with the Risk, Information Security, Compliance, Legal, HR, Physical Security, Operations, Finance and Internal Audit function on Data Privacy matters.
- Exchange regularly with the Operational Risk Management Function to ensure that the Data Privacy risk assessment is consistent with the Operational Risk Management's risk scenarios.
- Collaborate with the responsible business unit(s) to manage requests of Data Subjects including the rights of access, rectification and cancellation.
- Keep Senior and Business Management informed about their responsibilities with regard to Data Privacy.
- Attendance on the Data Protection and Security Committees.

Controls and Reporting

- Manage reporting Data Privacy requirements to relevant regulators, to Group, and to relevant parties.
- Manage Bharti AXA Life's relationship with, communications with, and reporting and submissions to the GDPO, regulatory and legal bodies.
- Attend inspections or queries raised by IRDA or any legal body with respect to data privacy
- Conduct an annual gap analysis against the Data Privacy Policy
- Report regularly the level of compliance of the entity to 1. the LMACC, 2. the Regional Data Privacy Officer, 3. the Group Data Privacy Officer , 4. the CEO and 5. Senior and Business Management of Bharti AXA Life.

Support and Expertise

- Supervise any Data Privacy related projects (e.g. BCR implementation).
- Define and communicate appropriate actions to reach Data Privacy compliance.
- Provide leadership and expertise on Data Privacy matters, including:
    - Act as the initial point of contact for any Data Privacy issues.
    - Provide expert advice on Data Privacy matters to the CEO, Senior Management, and all the areas and departments of Bharti AXA Life
    - Oversee training on Data Privacy matters is provided to all areas and departments of the Company and that the training is adequate and kept up-to-date.

- Provide guidance and adopt detailed requirements that provide greater emphasis on whether and how to process and manage Sensitive Personal Data;
- Provide guidance on how employees and non-employees can exercise any rights they may have under local law to complain about the way their Personal Data is being handled.
- Support on drafting Internal or external confidentiality agreements

- **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).
  - All data transfers involving personal/sensitive information shall be approved by the DPO

- **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/information, if required
  - Perform periodic audits of privacy, security and other necessary compliance activities to ensure overall legal compliance.

G. 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.

H. Personal Data Security Measures

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

- preventing unauthorised persons from gaining access to data processing systems for processing or using personal data (access control),
- ensuring that persons authorised to use a data processing system have access only to those data they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording (access control, need to know principle),
- ensuring that personal data cannot be read, copied, altered or removed without authorisation 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.

The level of the measures for data protection depends on the sensibility of the processing data. Data are classified in the Bharti AXA Life's Information security Policy. The data controllers are obligated to comply with Bharti AXA Life's ISM documents.

I. Awareness Measures

Persons incorporated in data processing shall not collect, process or use personal data without authorisation (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 familiarise persons incorporated in the processing of personal data with the recent legal provisions and special requirements of data protection.

Bharti AXA Life must ensure that employees, cooperative persons, contractors who work in AXA or any other relevant Third Parties are properly informed 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. Bharti AXA Life Data Privacy Policy shall also be made available on the website of the Company.

J. Principles for Data Transfer:

Sensitive 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 refer to the purpose of the transmission, the content of the data to be transmitted and the identity of the recipient.

Consent of the person concerned is not required:

- when the transfer is authorised by a law.
- when the data have been collected from publicly accessible sources.
- when the communication to be effected 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 Life or any person on its behalf may transfer sensitive personal data or information including any information, to any other organisation 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 organisation 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 Life or any person on its behalf and provider of information and where such person has consented to data transfer. Personal Data shall not be routinely transferred across borders without the written approval of the DPO.

K. Third Parties

o Providers of services

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.

o Rules for engaging suppliers

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.

L. 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 for sensitive personal data must be drawn up.

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

M. Control and Reporting

Bharti AXA Life would conduct an annual gap analysis against this Policy. The GDPO will provide the DPOs with a Gap Analysis Tool for that purpose.

The DPOs should exchange on a regular basis with the Operational Risk Management Function in order to ensure that their risk assessment is consistent with the Operational Risk Management's risk scenarios.

The DPOs are required to submit the annual gap analysis against this Policy to:

- the local Legal, Compliance or Risk Committee
- the RDPO (when existing)

A copy of the annual gap analysis shall be submitted to the local CEO and to the Senior and Business Management of the Company.

The annual gap analysis and a certification in relation to the Policy must be submitted by the DPO to the RDPO by 31st March for the preceding year.

N. Breach Reporting

A "Data Privacy breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

Usually, a Data Privacy breach happens when Personal Data (for example of clients or employees) is disseminated without authorisation, e.g. stolen, lost or mistakenly disclosed.

Bharti AXA Life would operate a Data Privacy breach reporting process to ensure that each incident is managed appropriately. This reporting process can leverage already existing reporting processes (for example the Events and Breaches reporting process).

Bharti AXA Life as required by local law and regulations would promptly notify affected individuals and/or the respective regulator and maybe the media when privacy is breached.

Under this Policy, Bharti AXA Life's business units are required to report breaches to the DPO, who in turn will decide and update the region.

Reporting to the Senior and Business Management, the DPO, the local CEO and the RDPO should be made within 5 working days of discovery of the breach. Reporting to the local Legal, Compliance or Risk Committee should be made at the next possible occasion.

O. Response to grievances or discrepancies

Bharti AXA Life shall ensure that any grievances or discrepancies faced by the provider of Sensitive Personal Data shall be addressed. A Grievance Officer shall be nominated who shall address the grievances or discrepancies raised by the provider of information within a month from the date of receipt of grievance. The Grievance Redressal Officer (GRO) shall act as the grievance officer for Bharti AXA Life, the name and the contact details of the Grievance Redressal Officer shall be made available on the website of the Company. Any grievances or concerns with respect to the usage of Sensitive Personal Data shall be sent to *head.customerservice@bharti-axalife.com.*

P. Records and References

- Regional Data Privacy Policy
- Information Technology Act, 2000 and The Information Technology (Amendment) Act, 2008
- Information Technology (Reasonable Security practices and procedures and sensitive personal data or information) Rules 2011