Policy Reference & Name : AEBC 69 India Data Protection Policy

Contents

1.0 OVERVIEW AND PURPOSE

The purpose of this document is to provide guidance on the ways American Express Banking Corp. (AEBC) meets its legal obligation for the protection of personal data in the India Market. We are committed to adhering to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the "Indian Privacy Rules")

The policy is to be read in conjunction with AEBC 47 Information Security Policy.

This Policy incorporates applicable legal and regulatory requirements as well as relevant regulatory guidelines. This Policy is subordinate to AEMP 48 – Privacy Risk Management Policy and incorporates the American Express ("AXP") Data Protection and Privacy Principles (Principles) contained therein. The standards of personal data protection set out in these Principles is used by AXP as a minimum standards globally, providing adequate and consistent protection for the processing of personal data. The latest Principles can be found on The Square and are also provided in the appendix of this Policy (in case of inconsistency, please always refer to the version on The Square.

This Policy supports, and does not supersede, AXP Information Security (IS) Policies and Standards. For more information regarding the IS Policies and Standards, please visit: Information Technology and Information Policy and Standards Global Standards Library.

2.0 SCOPE

This Policy applies to all business units and colleagues of AEBC and its Businesses. This Policy covers various aspects of personal data protection, including:

1. Collection
2. Notice and Processing
3. Choice
4. Data Quality
5. Security and Confidentiality
6. Data Sharing
7. Openness and Data Access
8. International Transfer
9. Responsibility
10. Accountability

This Policy does not apply to "business contact information" which is defined as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his/her personal purposes."

3.0 KEY DEFINITIONS

TERM	DEFINITION
India Data Protection Program	The Data Protection compliance program designed by AEBC India Compliance & Ethics
Data Protection and Privacy Principles	Data Protection and Privacy Principles set out the way that AXP and its wholly owned direct and indirect subsidiaries will collect, use, store, share, transmit, delete, or process customers' personal data.

AXP Global Privacy Policy Framework	The AXP Global Privacy Policy Framework guides the conduct of American Express and its wholly owned direct and indirect subsidiaries in the 'processing' of personal data. AXP business units operate within that Framework and have policy documents that are fully consistent with the AXP Data Protection and Privacy Principles and are available on The Square.
Behavioral Advertising	Targeting specific marketing offers and promotions based on a Web user's on-line habits / interests
Business Contact Information	An individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, unless the personal data was provided by the individual solely for use in a personal context
Confidentiality	Ensuring that information is accessible only to those authorized to have access
Consent	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her
Cookies	A text file created on the computer when a user first visits certain web sites. Cookies store user information which, among other things, potentially can be used in Behavioral Advertising
Regulators	AEBC may be required to furnish details of Information Providers as required by law to Reserve Bank of India
Market Compliance Office (MCO)	Overseeing the implementation of and ongoing compliance with the Data Protection Policy with support from GPO and serves as the main point of contact for communication with regulatory authorities
Data Quality	The accuracy, completeness, and relevancy of information
Data Security	The means of ensuring that data and / or information is protected from corruption (Integrity), destruction (Availability), and/or disclosure (Confidentiality)
Data Sharing	The disclosure of data from one or more organizations and/or individuals to a third-party

	organization, or the sharing of data between different parts of an organization
Privacy Risk Management Policy (AEMP 48)	The policy which describes how AXP manages privacy risk on an enterprise-wide basis. Core to the Privacy Risk Management Policy are the AXP Data Protection and Privacy Principles
Global Records Management Policy (AEMP 08)	The policy which refers to the way in which AXP should retain only those records that are required for effectively running its business operations and to satisfy its obligations to customers, colleagues, legal and regulatory authorities and shareholders
Information Security (IS)	Office responsible for Information Security strategy and activities throughout the American Express Organization
Outsourcing / Outsourced arrangements	Any functionality or process that has been contracted to a third party, whether or not within the AXP group of companies (see third party). This could include, but is not limited to, telephone servicing, account acquisition via an agent who is also collecting personal data and performing identity checks on AEBC's behalf or retaining data with an off-site records storage facility.
Personal Data	Personal Data refers to information, in any form, that identifies or can be used in combination with other information available to the Company to identify an individual and includes any information that is associated with an identified individual.
Privacy Choice	Giving individuals the opportunity to determine, in certain circumstances, what information about them AEBC can collect, use, and with whom AEBC can share it. Specifically, privacy choices provide a customer with the opportunity to determine how, or whether, to be contacted for Marketing (by phone, mail, email etc.) Some of these choices are dictated by applicable law; some are driven by AEBC's commitment to meet its customers' desire to protect their Privacy. Privacy Choices captured by AEBC include: • Use of Card Member information for offers of third-party products and services • Use of Card Member information for AEBC direct mail offers • AEBC Telemarketing offers

	• AEBC Email offers
Privacy Notice	Notice is the clear and appropriate disclosure to individuals of who we are and how we collect, use and share personal data. It is a promise to our customers of how we will treat their personal data. A Privacy Notice is a legally binding agreement. Different American Express Business Units may issue separate Privacy Notices. Online, we make a similar promise to our customers in the form of our online Privacy Statement. A Privacy Notice always contains three key elements: • What personal data we want to collect • How we intend to use it • With whom we intend to share it
Global Privacy Oversight	The Global Privacy Oversight is responsible for supporting the privacy program and managing privacy risk of data covered under AEMP 48 or its Global Policy Framework. GPO serves as the main point of contact for privacy-related questions
Processing	Any operation performed on personal data from customers and/or colleagues, e.g. collect, use, store, share, transmit, delete or otherwise process.
Standards	Derived from generally accepted industry standard frameworks, a specific set of rules that are designed to structure and guide implementation of policy and allow an organization to operate uniformly and effectively; a set of auditable minimum requirements that support policy objectives.
Third Party	A non-affiliated company/individual with which AEBC partners and which is not part of the American Express Group of Companies. This includes Merchants, Publishing Advertisers, Authorized Service Providers and other non-merchant business partners.

4.0 ROLES & RESPONSIBILITIES

The AEBC Risk Committee is primarily responsible for overseeing the control environment throughout the organization. The Committee acknowledges and supports the strategic importance of data protection and privacy and recognizes the importance of an effective Privacy Program, and its success in terms of meeting American Express expectations as well as legal and regulatory requirements.

The AEBC Market Compliance Officer ("MCO") is responsible for overseeing that this Policy is developed and embedded into AEBC's day-to-day operations. The MCO, which is the second line of defense, provides oversight, support, and governance for privacy risk management.

The **General Counsel's Office** provides data protection legal requirements, interpretation, and guidance to privacy risk stakeholders.

The Global Privacy Oversight ('GPO") reports to the AXP Chief Privacy Officer (CPO) within the Chief Risk Officer's organization. The GPO in conjunction with Operational Excellence and the Business Units, are responsible for ensuring that all requisite components of the privacy risk management program are implemented in business units. The Global Privacy Oversight also provides strategic guidance to the business on privacy risk management strategies, best practice controls and processes.

The GPO responsibilities also include privacy risk oversight functions. The GPO is accountable for privacy risk oversight, breach notification, monitoring and governance across the enterprise and manages the overall AXP Privacy Program framework. The GPO partners with Compliance to ensure privacy compliance risks (which are managed through the Global Legal Inventory and Compliance Program activities) are incorporated into the Global Privacy Program for holistic and global privacy risk management.

In some markets representatives from the Global Privacy Oversight serve as the appointed regulated entity Privacy Officers and/or Data Protection Officers (DPO) such as in the United States and Europe. In other markets, the GPO partners, and coordinates with appointed regulated entity Privacy Officers or DPOs or MCO in Compliance to promote consistency of privacy operational requirements with specific regulated entity and market rules.

The Information Security Office is responsible for defining the Information Security policies and standards on behalf of American Express.

Business Unit Presidents decide on and own privacy risk acceptance and mitigation with guidance from Operational Excellence and the GPO. BUs are responsible to implement the global privacy risk management program, which includes the implementation and testing of privacy controls to meet the requirements of privacy policies and standards and the Company's operational risk framework (e.g. privacy controls for Process Risk Self Assessments), and the remediation of privacy risk events, including issues or events associated with the business' use of global privacy capabilities.

5.0 REQUIREMENTS UNDER THE PERSONAL DATA PROTECTION POLICY

The *"Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011"* comprises various rules governing the collection, use, disclosure and care of personal data. It recognizes both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes.

Disclose Personal Information to credit reporting agencies before, during or after providing credit to you as per the Credit Information Companies (Regulation) Act, 2005. This includes, but is not limited to:

- that you applied for a Card and the credit limit, and that we are a credit provider to you;
- report about your Card payments on an ongoing basis and which are overdue, and which are in collection (and advice that payments are no longer overdue);

5.1 Data Collection

AEBC must collect personal data from customers and individuals in a fair and lawful manner.

Specifically, AEBC will:

- Collect only as much personal data as is required for its business purpose.
- Collect personal data in a fair and reasonable manner;
- Notify the individuals, at the time of collection, the purpose of the collection, use or disclosure of personal data;
- Collect personal data directly from the individual, where possible, and;
- Verify that personal data collected from third parties is reliable and lawfully provided;

What Personal Information do we collect?

We collect various types of Personal Information from you such as your name, address, telephone number, mobile number and email address. Collecting this Personal Information enables us to offer you services, online experiences that help you with your financial and payment needs, fulfill our obligations as an employer, conduct our business with our merchant, vendor, partner, customer or any other Information Provider. Depending on the nature of the relationship, we also collect information such as your date of birth, employment details, tax file number, etc.

What Sensitive Personal Information do we collect?

Depending on the nature of the relationship, we may collect some limited Sensitive Personal Information such as information about your credit history, bank account details, financial information, your account number, passwords, etc.

We will only collect Sensitive Personal Information with your consent. You can always withdraw their consent (see Principle 8 – Choice for details).

We do not generally collect information about your health, medical condition, sexual orientation, religion, ethnic origin or political associations.

How do we collect Personal Information?

Generally, we collect Personal Information directly from you. However, we may also collect Personal Information about you from third parties such as:

- Credit bureaus and agencies;
- Merchants (when you make purchases with your card or account);
- Referees; and
- Publicly available information sources (such as social networking sites, etc.)
- Our Vendors and/or our affiliates such as American Express Services India Limited and American Express India Private Limited

Marketing

We record information about your transactions and how you interact with third parties like a utility or phone company. We use this information in combination with other information we may have in order to better tailor and personalize our services and for marketing purposes. For example, we may use marketing segments developed by us or other companies to customize certain services to your local area and provide relevant offers tailored to you.

More information about collection

If you would like to know the name and address of agencies collecting and retaining your Personal Information, please contact our Grievance officer (see Principle 9 – Accountability for details).

5.2 Privacy Notice

AEBC must notify individuals about the purposes for which it collects, uses or discloses personal data about them.

AEBC India must, at the time of collection of personal data, notify the individual of:

- The American Express legal entity that is collecting the personal data (i.e. AEBC)
- The type of personal data collected;
- The purpose for which this personal data is collected;
- How the personal data will be used or processed;
- Whether the personal data will be collected by or disclosed to third parties (a statement of this fact and the purposes for doing so);
- How individuals can access their personal data and correct or delete it if it is inaccurate, and
- How to contact AEBC and its Grievance Officer with questions, corrections, complaints, or disputes.

If AEBC intends to use such personal data for a purpose other than for the original purpose, AEBC needs to inform the individual of those purposes and obtain consent.

Generally, we collect and process Personal Information for the following purposes:

- To process your application for an account or service
- To manage and service your account
- To research and develop new products and services
- For training, quality control purposes
- To manage competitions, offers or promotional campaigns you have entered
- To authenticate your identity
- To communicate with you and to contact you with offers from time to time
- To meet our legal and regulatory obligations
- To process your job application
- To fulfill our obligations as an employer, conduct our business with our merchant, vendor, partner, customer or any other Information Provider

In providing your email address, telephone and facsimile numbers you are agreeing that we may contact you by email, telephone or facsimile.

5.3 Choice and Consent

All Information Providers have the option to withdraw their consent provided to us, you may also approach the Grievance Officer. However, in such cases we may not be able to provide you with the services for which the Personal / Sensitive Information was provided. For example, this may mean we need to cancel your card account or terminate your employment with us.

AEBC may collect, use or disclose personal data only with the individual's knowledge and consent. In this regard, AEBC must obtain consent from individuals, when:

a) Personal data collected from an individual;

b) When personal data is disclosed by AEBC to a third party (other than service providers) or,
c) If personal data is to be used for a purpose that it was not originally intended for.

In addition, AEBC must provide individuals with the opportunity to opt in or out from their personal data being processed for Marketing purposes.

Telemarketing

For telemarketing, Card Member can choose the manner to receive marketing communications, including direct marketing - whether AEBC send them through postal mail, email, SMS and/or telephone. If Card Member chooses to not receive marketing communications from AEBC, the request will be adhered. AEBC can still communicate with Card Member through servicing mailers, fulfilling the requests, fulfilling any regulatory requirement, or administering any promotion or any program in which Card Member have elected to participate.

Telecom Regulatory Authority of India (TRAI) has issued a guideline the Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018 to curb Unsolicited Commercial Communication (UCC). Under this regulation Bank is required to send SMS every 6 months to its existing base of CMs renewing their consent recorded to receive marketing communication.

5.4 Data Integrity and Data Quality

AEBC must have reasonable processes in place to keep personal data accurate, complete, and up to date, for the purpose for which it was collected.

The following Information Security Policies and Standards apply to AEBC operations:

- Information Ownership and Classification Policy (AXP-IS04)
- Information Ownership and Classification Standard (AXP-IS04.01)
- Information Handling and Disposal Standard (AXP-IS04.03)
- Access Control Standard (AXP-IS09.01)
- Third Party Management Standard (AXP-IS16.01)

For more information regarding the IS Policies and Standards, please visit: Information Security Policies and Standards Library

5.5 Data Use and Data Retention (Record Retention)

AEBC must collect, use, process, store, and/or retain personal data only for legitimate business purposes, and only for as long as it is required for those purposes. AEBC as an organization shall cease to retain personal data as soon as personal data is no longer needed for the purpose which it was collected, or the retention of the personal data is not necessary for legal or business purposes.

Specifically, AEBC will use, store, and/or process personal data consistent with:

- The purpose for which it was collected,
- Appropriate consent being obtained,
- Contractual terms applicable for business partner / client relationships,
- AEBC policy and procedures; and
- Applicable legal requirements and regulatory guidelines.

Personal data must be retained and / or destroyed according to AXP Global Records Management Policy (AEMP 08) and AXP Enterprise Records Retention Schedules, guidelines and data destruction procedures.

We destroy all Personal Information that is no longer needed for the purposes for which we collected it, unless its retention is required to satisfy legal, regulatory or accounting requirements or to protect our interests.

Data purge capability must be implemented in different system databases to remove or anonymize personal data upon expiry of retention period. For details of the policies and procedures for data retention, please go to Enterprise Records Management on The Square.

5.6 Data Security

AEBC must take reasonable precautions and have appropriate procedures in place to safeguard personal data against loss, misuse and un-authorized access, disclosure, alteration, destruction, and theft.

AEBC has information security policies and standards that address the following areas and include:

- Clear desk procedures
- Secure work area instructions
- User access controls on information systems
- Secure filing mechanisms for records containing personal data of individuals
- Documented record retention procedures (as covered in Section X)
- Documented data destruction procedures
- Record keeping procedures for data destruction (certificates)
- Backup and storage of Information (so called, Business Continuity Planning)
- USB drive usage

AEBC colleagues are required to:

- Protect sensitive information and prevent its loss or disclosure to unauthorized parties;
- Prevent any unauthorized use of personal/sensitive information;
- Comply with applicable legal requirements and regulatory expectations
- Protect customer/colleague personal data at all times.
- Ensure that transmission of customer/colleague personal data must be encrypted according to the Information Security Policies and Standards

Basis the updated Master Direction – Know Your Customer, Aadhaar is not a mandatory requirement while applying for a credit card. Hence, if an applicant still wants to provide his/her proof of possession of Aadhaar as OVD, Bank has made a process to accept the Aadhaar only if the first 8 digits of Aadhaar number are masked.

Sensitive Personal Information does not include information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force.

The AXP Information Security (IS) organization has developed and implemented global Information Security Policies and Standards, applicable also to India operations, such as:

- Information Ownership and Classification Policy (AXP-IS04)
- Information Handling and Disposal Standard (AXP-IS04.03)
- Access Control Standard (AXP-IS09.01)
- Third Party Management Standard (AXP-IS16.01)

These policies and standards can be found on The Square at: Information Security Policies and Standards Library

5.7 Privacy Breach Incident Reporting

The AXP Enterprise Incident Response Program (EIRP) is a key component of the Information Security Program's efforts and manages the data breach lifecycle from identification to notification associated with potential privacy or security breaches of

- Personal Data relating to current, former and prospective customers and colleagues
- AXP proprietary information
- AXP systems

In accordance with the AXP Security Incident Reporting Policy (AXP-IS06) and the AXP Security Incident Reporting Standard (AXP-IS06.01), AXP colleagues must immediately report any incidents of suspected data breaches to the EIRP.

Chief Information Security officer (CISO) is responsible for reporting Incidents to the regulator. Kindly refer to AEBC 47 Information Security Policy and AEBC 43 Cyber Crisis Response Policy available on The Square for more details related to Enterprise Incident Response Program

5.8 Data Sharing

Under the AXP Data Protection and Privacy Principles, generally we share your Personal Information with the following:

- Regulators
- Lawyers
- Auditors
- Any agent, contractor or third-party service provider who provides administrative, telecommunications, computer, payment or securities clearing or other services in connection with the operation of its business;
- Any other person under a duty of confidentiality to us
- The drawee bank providing a copy of a paid cheque (which may contain information about the payee) to the drawer;
- Credit reference agencies and, in the event of default, debt collection agencies;
- Any actual or proposed assignee of or participant or sub-participant or transferee of our rights in respect of the data subject.
- Our business alliance partners.

AEBC shall only share personal data with third parties where:

- it is necessary to provide customers with products or services;
- it is in connection with AEBC efforts to reduce fraud or criminal activity (subject to the individuals being informed of the purpose of data disclosure); or
- it is permitted by law.

Where any personal data is collected, a disclosure on the sharing personal data with a third party must be clearly documented in writing.

When sharing information with third parties AEBC must:

- Provide notice and obtain consent from individuals, as applicable,
- Ensure that access to data can only be processed as described in notice,
- Only disclose personal data to third parties for the purposes identified in the Notice provided to individuals, and only disclose as much information as is required for the purpose,
- Share personal data in a way that is fair and consistent with the rights of the individual whose information is being shared,

- Verify that actions align with the consent provided by the individual, in addition to any applicable legal and/or regulatory requirements,
- Require third parties, through contractual clauses and/or written agreements, to adhere to AXP applicable Privacy, Data Protection and Information Security Controls,
- Require third parties to process personal data in accordance with the individual's Privacy choices and consent obtained from the individual, as legally required;
- Ensure that the third party only acts on the instructions provided by AEBC; and
- Ensure that the third-party colleagues are duly trained on the requirements as set out herein.

Subject to the Privacy Rules, we and our agents may share Personal Information as follows:

Information Sharing	Nature of information and purpose:
Co-brand partners	Provide Personal Information to any organization whose name, logo or trademark appears on customer's application for the Card or on the Card issued to customer, for marketing, planning, product development, and research and management information purposes.
Marketing lists/data with 3rd parties	Use Personal Information for marketing purposes. This includes putting customer's name and contact details as on marketing lists for the purposes of customer research and offering goods or services of us or of any third party, by mail or email or having our related companies do so directly
Our service providers	Transfer Personal Information in a secured manner to our related companies and other organizations. This includes transferring Personal Information to the United States or other countries for data processing and servicing.
Call monitoring	We may monitor and record telephone conversations with us from time to time for training, quality control or verification purposes
Information from credit reporting agencies	Obtain credit reports about customer from credit reporting agencies to assess customer's application or to collect overdue payments from customer, and obtain Personal Information from a business that provides commercial credit worthiness information
Regulators	American Express Banking Corp. may be required to furnish details of Information Providers as required by law and to fulfill the obligations. Pursuant to the G.S.R. 313(E) notification, American Express Banking Corp. will ask the government authorities to not share the information provided to them by American Express Banking Corp., with anyone without its permission.
Credit providers	Exchange Personal Information with credit providers named in customer's application or in a credit report issued by a credit reporting agency. This is for purposes including but not limited to: • assessing customer's credit worthiness, customer's application for the Card and for any subsequent application customer make for credit; • notifying other credit providers of customer's default or failure to comply with these conditions; • exchanging information about customer's Card account where customer is in default with other credit providers; • approving or declining a transaction customer wishes to make with the Card; and – our administration of customer's account.

Persons, you tell us about	Exchange Personal Information with any person whose name customer give us from time to time. This includes, for example, for the purpose of confirming customer's employment and income details with any employer, landlord/mortgagee, accountant, financial adviser or tax agent details of whom are received by us along with customer's application for the Card.

Collection agent	If you are in default under the Card account, notify and exchange Personal Information with our collection agent.

Where information sharing is between AEBC LOBs, each LOB must review its own terms and conditions to ensure that it covers such sharing and obtain confirmation from AEBC Compliance Team that such sharing does not contravene our obligations under Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

Details of policy requirements and Data Privacy Principles are attached at Annexure A.

Data Privacy Principles shall also be available on American Express India website at https://www.americanexpress.com/in/legal-disclosures/privacy-principles.html

Outsourced Operations

Outsourced arrangements/service providers handling and processing personal data of AEBC, its customers, clients and colleagues shall be responsible for securing such information in accordance with this Policy, AXP Information Security Policy and Standards, as well as applicable laws and regulations. All service providers/third parties handling personal data are also required to sign up to AXP Information Protection Contract Requirements ("IPCR"). Please consult IS for guidance on the IPCR or visit Information Protection Contract Requirements on The Square.

AEBC Business Unit Directors and assigned Relationship Managers are responsible for ensuring that each third-party relationship operates in accordance with this Policy.

Colleague Data Sharing

Under the American Express Privacy Standard, AXP will not share current and former colleague, applicant for employment, contingent worker and/or contractor personal data with third parties and/or vendor partners, unless legally required or for purposes of employment related processing/servicing (e.g., healthcare, payroll/benefits administration, etc.) or internal investigation.

5.9 International Transfer

Personal data relating to AEBC customers, clients and colleagues may only be transferred to AEBC Business Units in the United States and other countries, per local Country regulatory requirements and the application of AXP Global Information Security Standards and Policies. Appropriate Data Protection statements are also included in AXP products' Terms & Conditions and Privacy Notices, as applicable.

When transferring personal data outside of India AEBC must:

- Ensure such data transfer is necessary for the performance of the lawful contract between AEBC and provider of data/information or ensure that provider of data/information has consented to such data transfer.
- Ensure that the country to which personal data is transferred has an adequate level of Data Protection
- Ensure that local Data Protection and Privacy requirements have been met prior to data transfer.

5.10 Complaints and Dispute Resolution

AEBC must:

- Make information available on request about AEBC Data Protection and Privacy related practices and where and how to raise enquiries or concerns;

- Immediately inform the Grievance Officer about any data privacy related complaint;

- Formally acknowledge, document, investigate, address and respond in a timely manner any formal Data Privacy complaints in accordance with the India Complaint Management Policy

AEBC colleagues must report all potential, apparent or actual violations of this Policy to their leader or the AEBC Grievance Officer. Alternatively, any concerns can be raised confidentially to the Amex Ethics Hotline at: https://amex.ethicspoint.com/

5.11 TRAINING

All AEBC colleagues shall undertake annual Information EET-I Information Security Awareness, Code of conduct and Data Protection and Privacy Training as mandated by AEBC. Contractors, vendors and partners that have access to restricted and secret customer, prospective customer, client and colleague data that is personally identifiable must also take these trainings.

Senior Leaders, Marketing and Sales colleagues and staff in operational areas may also be required to undertake specific training on areas relevant to their roles, such as requirements for electronic communications, use of cookies and behavioral advertising.

AEBC must conduct training and review its compliance with these Privacy Principles. Employees who violate these Privacy Principles may be subject to disciplinary action, up to and including dismissal. Employees are expected to report violation of these Privacy Principles, and may do so to their managers, to the MCO, to the General Counsel's Office (GCO), to the Grievance Officer or to the Amex Ethics Hotline at: https://amex.ethicspoint.com

6.0 POLICY EXCEPTION/ CONFLICT/ INTERPRETATION RESOLUTION

It is the responsibility of American Express employee subject to this policy to escalate to the Policy Sponsor or Policy Overseer any conflicts, interpretation issues, or policy gaps/inadequacies associated with AEBC Policies. The Policy Custodian may provide policy interpretation and guidance as needed; but when potential issues have contradictory interpretations for existing practices the Custodian should facilitate a discussion with the Policy Sponsor and Overseer to develop appropriate resolution plans.

All requests for exceptions to policies, or the related procedures, must be formally approved by the Policy Approvers, as outlined in Section 7 of this Policy. Exception requests must include an Action Plan and Rationale and must carry either an Expiration or Review Date. Any identified exception to a policy that has not yet been approved must be escalated to the respective Policy Overseer immediately. Approved policy exceptions do not constitute policy non-compliance.
It is the responsibility of the Policy Sponsors to define their Policy's Exception / Conflict / Interpretation Resolution Requirements. The Policy Custodian will maintain documentation of all exceptions and will regularly review these exceptions to assess whether a policy change is required and to ensure ongoing policy compliance.

The AEBC CRO retains the authority to resolve conflicts only surrounding policy framework related matters, with appropriate senior leadership, should they arise.

7.0 POLICY APPROVAL REQUIREMENTS

This policy must be reviewed and approved by the AEBC CEC at least biennially. Additional reviews could be triggered by major changes in corporate strategy, the regulatory environment or financial market conditions.

Prior to each review by the AEBC CEC, this policy, and any proposed changes in this policy, should be reviewed by:

Approval Level

Level 1	N/A
Level 2	AEBC CEC and AEBC RMC
Level 3	N/A
Level 4	Policy Sponsor – AEBC Chief Compliance Officer
	Policy Overseer – N/A (Second Line Policy)

8.0 ENFORCEMENT OF ISSUED POLICIES AND PROCEDURES

All employees and agents of AEBC are responsible for complying with applicable official policy, procedure or a standard/program. AEBC Senior Management and Officers are ultimately responsible for ensuring adherence to policy within AEBC. Internal auditors and control groups, as applicable, will review compliance with policy and procedure. **Noncompliance with issued policies or procedures is a breach of the terms of employment and may lead to disciplinary actions which may include termination of employment, or third-party agreement.**

AEBC Policies do not take precedence over local law, yet still must be aligned to management policy requirements.

9.0 POLICY IMPLEMENTATION

Management will oversee that procedures necessary to implement this policy are established for. The policy is effective as of the date on the cover page.

10.0 RELATED POLICIES, GUIDELINES AND SUPPORTING DOCUMENTS

This Policy is in addition to (and supplemented by) following AEBC policies, including:

- AEBC 7.18 India General Compliance Policy
- AEBC 7.25 India Protected Disclosures Policy
- AEBC 5.01 Information Security Policy and
- AEBC 5.09 Cyber Crisis Response Policy

11.0 REVISION HISTORY

S/N.	Date	Change Description
1.	January 2019	• Formatting changes • Reference of Information Technology Act and Rules 2011 • Defined opt in/ opt out option available to CM for telemarketing communication
2	January 2021	Insertion of below details: • Requirement under The Telecom Commercial Communication Customer Preference Regulations Regulation • Masking of Aadhaar number • Role of CISO under EIRP process Deletion of below details: • Para on Data Access
3	March 2021	• Deletion of Local Data Privacy Officer reference as no such local requirement • Change in name of Grievance Officer
4	March 2023	• Update references to Global Privacy Office to Global Privacy Oversight. • Clarity added on international data transfer

12.0 APPENDICES

APPENDIX A – AXP Data Protection and Privacy Principles

Data Protection and Privacy Principles

Effective: May 15, 2018

The following Data Protection and Privacy Principles ("Principles") set out the way that American Express Company and its wholly owned direct and indirect subsidiaries ("American Express") will collect, use, store, share, transmit, delete or otherwise process (collectively "process") your personal data. Personal data means any information that relates to an identified or identifiable individual. The standard of personal data protection set out in these Principles will be used by American Express globally, providing adequate and consistent protection for the processing of your personal data.

These Privacy Principles cover Personal Information that we collect in India directly from:

• "Information Providers" including but not limited to Customers, Merchants and Employees of AEBC India.

In these Principles, "you" and "your" means any individual customer or employee of American Express and any other individual whose personal data we process and "we", "us", "our" and "American Express Group" means American Express.

What Information is covered by these Privacy Principles?

We collect both Personal Information and Sensitive Personal Information in India.

In these Privacy Principles, the term "Personal Information" 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.

In these Privacy Principles, the term "Sensitive Personal Information" means Personal Information that also consists of information relating to:

• Passwords

• 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

Sensitive Personal Information does not include information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force.

Collection

We will only collect personal data that is needed and by lawful and fair means.

Notice and Processing

Where it is not apparent from the products or services you require or the nature of your relationship with us, we will tell you how your personal information and Sensitive Personal Information will be processed and which partners or vendors are responsible for that processing. We will process your personal data fairly and only for those purposes we have told you, for purposes permitted by you and retain/store as permitted by applicable law. In addition, you may object to certain types of processing as expressly permitted by applicable law.

Choice

We give customers the option of having their personal data included or removed from lists used for marketing as required by applicable law. This includes product and service offers from American Express and those made in conjunction with our business partners. Of course, each of our businesses will continue to send customers information about the products or services they receive from that business.

Data Quality

We use appropriate technology and well-defined employee practices to process your personal data promptly and accurately. We will not keep your personal data longer than is necessary, except as otherwise required by applicable law.

Security and Confidentiality

We will keep your personal data confidential and limit access to your personal data to those who specifically need it to conduct their business activities, except as otherwise permitted by applicable law. We refer to industry standards and use reasonable administrative, technical, and physical security measures to protect your personal data from unauthorized access, destruction, use, modification, or disclosure. We require industry standard data security measures from those third parties who are authorized by us to process your personal data on our behalf.

We use 128-bit digital certificate from Verisign for encryption of the Secure Sockets Layer (SSL) session which is an industry standard for encryption over the internet to protect the data of users. 128bit-SSL is the highest level of commercially available security for encrypted communication. When you type in Sensitive Personal Information such as credit card details, it will be automatically converted into codes before being securely dispatched over the internet. We require industry standard data security measures from those third parties who are authorized by us to process your Personal Information on our behalf.

Data Sharing

We only share your personal data with third parties where it is necessary to provide you with products or services or as part of the nature of our relationship with you, where we have previously informed or been authorized by you, in connection with our efforts to reduce fraud or criminal activity, or as permitted by law.

Openness and Data Access

If you ask, we will inform you about how your personal data is processed and the rights and remedies you have under these Principles. You may inquire as to the nature of the personal data stored or processed about you by American Express. In accordance with the Information Technology (Reasonable security practices and procedures and sensitive Personal Information or information) Rules 2011, you will be provided access to Personal Information about you held by us. If any data is inaccurate or incomplete, you may request that the data be amended.

International Transfer

Where it is not apparent from the international products or services you require or the nature of your relationship with us, we will inform you if your personal data may be transferred outside of your country and ensure that such transfer is only performed in accordance with applicable law. Regardless of where your personal data is transferred, your personal data is protected by these Principles.

Responsibility

Each company in the American Express Group and their employees may only process your personal data in accordance with these Principles. We conduct training and reviews of our compliance with these Principles. Employees who violate these Principles may be subject to disciplinary action, up to and including dismissal. Employees are expected to report violation of these Principles, and may do so to their managers, to their business unit's compliance officer, to the legal department, to the Global Privacy Oversight or to the Amex Ethics Hotline.

Accountability

You may enforce these Principles in your country against any company in the American Express Group that is responsible for your personal data, as a third-party contractual beneficiary to these Principles. If you have a complaint that we have breached these Principles and have attempted in good faith to resolve the complaint through our customer service process, but the complaint was not resolved by us within a reasonable amount of time, then you may enforce these Principles against us. If you feel that we have breached these Principles, you are entitled to bring a complaint to our Grievance Officer (See details below) If we fail to resolve your complaint within one month, then you may enforce these Privacy Principles against us by taking your complaint to your local data protection authority. We will abide by the findings of the data protection authority, but we reserve the right to challenge or appeal such findings. These Principles do not affect any rights you have under applicable law, the requirements of any

applicable regulatory data protection authority, or any other type of agreement that you may have with us.

These Principles emphasize our commitment to protect your personal data. They are binding on all companies in the American Express Group, demonstrating our commitment to privacy. In addition, each company in the American Express Group that holds personal data may maintain its own additional rules and practices for products or services, consistent with these Principles.

If you have questions or comments about these Principles, please contact us at American Express.

Grievance Officer

Any concerns, disputes, discrepancies, or grievances with respect to processing of Personal Information can be referred to the designated Grievance Officer, as below:

Name: Mr. Saurabh Khanna

Address: American Express Banking Corp. Cyber City, Tower C, DLF Bldg. no.8, Sector-25, DLF City Ph II, Gurgaon, Haryana-122002, India.

Email ID: **AEBCNodalOfficer@aexp.com**.

Telephone no: 0124-6702638

The Grievance Officer shall redress the grievances within one month from the date of receipt of grievance.