አዋሽ ባንክ
AwashBank

DATA PRIVACY POLICY

October 2021

Acronyms

AB	Awash Bank
BODs	Board of Directors
CEO	Chief Executive Officer
KYC	Know Your Customer
NBE	National Bank of Ethiopia
SME	Small and Medium Enterprise

Table of Contents

SECTION ONE

INTRODUCTION

1.1 Background

Data about customer needs to be captured for KYC and similar purposes. It shall be stored properly and retrieved as and when required. Here, data privacy is very crucial. Data privacy, sometimes also referred to as information privacy, is an area of data protection that concerns the proper handling of customer's sensitive data including personal and other confidential data, such as certain financial data, to meet regulatory requirements as well as protecting the confidentiality and immutability (non-changeability) of the data.

Banks and other financial institutions manage a large volume of sensitive information about their customers, and the breach of such data can have dire consequences. For these institutions, customer data privacy is not just a key competitive advantage, but a precondition for existence on the business market.

International and industry-specific mandates for personal and financial data protection are applicable to all banks that handle financial data, either as data controllers or data processors. In Ethiopia, Financial Consumers Protection Directive No. FCP/01/2020 of NBE requires data protection by financial services providers.

AB realizes the need for a well-defined data privacy practices to ensure secured services to all customers within the prescribed regulatory framework. In this regard, data privacy issues have been part of many policies and procedures that relates to customers in one way or another. But a separate Data Privacy Policy has been required by the NBE. Thus, in line with the requirement of NBE, considering current banking environment, rules and regulations of the country, this Data Privacy Policy is prepared.

1.2 Objective of this Policy

The general objective of this Policy is to create a harmonized system of management of data privacy activities in the Bank in accordance with applicable laws and regulations. Specifically, this Policy aims at:

a) Providing a comprehensive guidance for the Bank's activities related to Data Privacy,
b) Providing an improved understanding as to the characteristics of Data Privacy activities,
c) Serving as a tool for safeguarding the Bank and its customers,
d) Encouraging and facilitating secured services to customers.

1.3 Scope of this Policy

This Policy governs issues of Data Privacy activities such as, collection of data, data storage, data protection, access of data, use and disclosure of data, data disposal, awareness, training and support for data privacy.

1.4 Definition of Terms and Concepts

Agent: refers to a person appointed and contracted by the Bank to act on behalf of a Bank and for a commission in a manner specified by the relevant directives of the National Bank.

Confidentiality: refers to protecting data, objects and resources from unauthorized viewing and other access.

Customer: refers to an entity who uses products and services of a bank.

Data: refers to any information about an identified or reasonably identifiable customer.

Data Disposal: refers to the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes.

Data Encryption: refers to the process of conversion of data from a readable format in to an encoded format that can only be read or processed after it's been decrypted.

Data Privacy: refers to the practices which ensure that the data shared by customers is only used for its intended purpose.

Data Protection: refers to the process of safeguarding important information from corruption, compromise or loss.

Disaster Recovery: refers to a continuation of vital technology infrastructure and systems following a natural or human induced disaster.

Data Retention: refers to the continued storage of an organization's data for compliance or business reasons.

Data Storage: refers to the recording (storing) of information (data) in a storage medium.

Personal Data: refers to information that relates to an identified or identifiable entity.

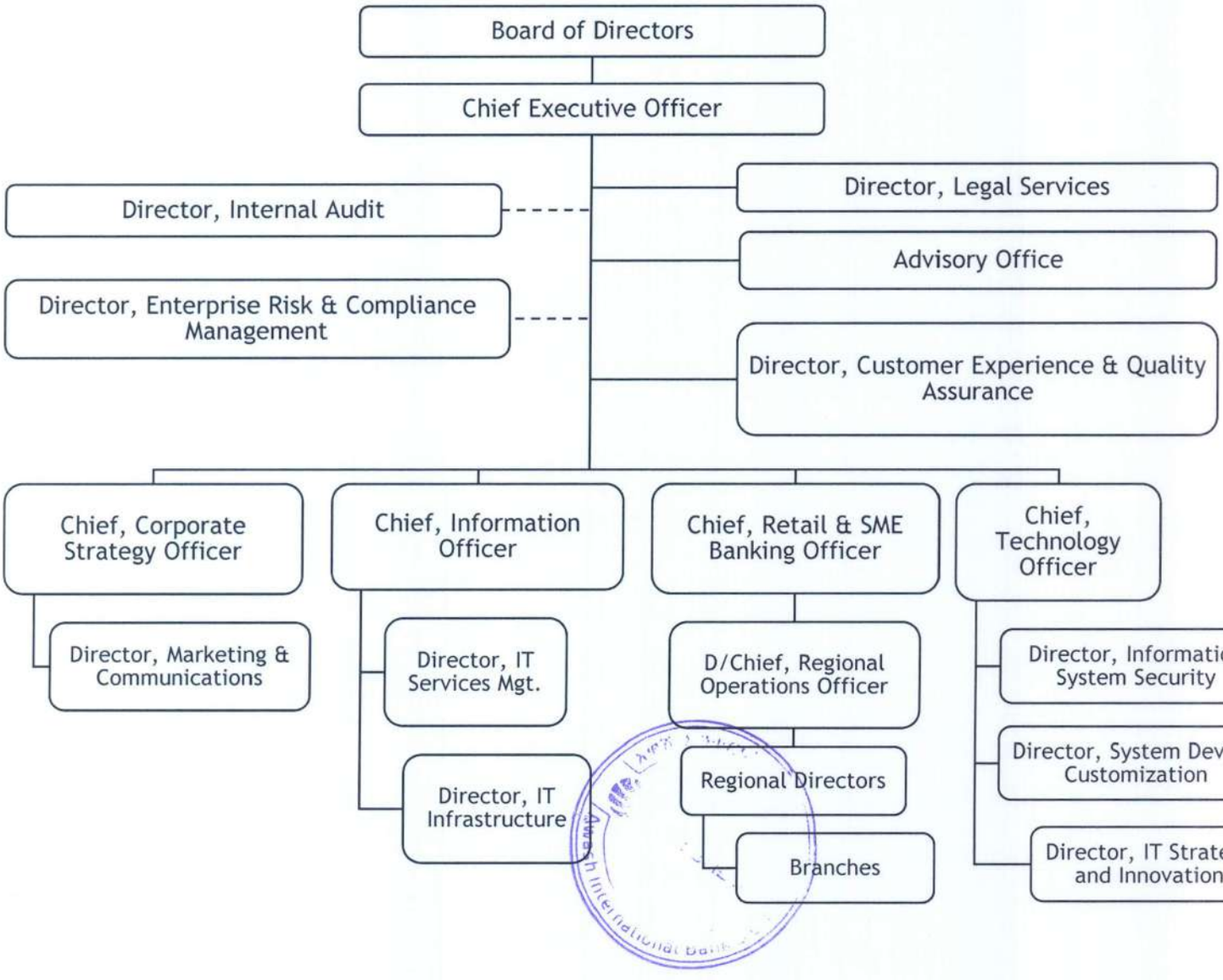
Third Party: refers to an entity who is outside of or not a direct party to the contractual relationship between the Bank and customer.

SECTION TWO

ORGANIZATIONAL STRUCTURE, ROLES AND RESPONSIBILITIES

The organizational structure, roles and responsibilities of various organs of the Bank as related to the management of Data Privacy activities are as indicated below.

2.1 Organizational Structure



2.2 Roles and responsibilities

2.2.1 Board of Directors

The major roles and responsibilities of the Board of Directors in the management of data privacy related activities are;

a) Review & approve data privacy policy.
b) Oversee the existence of adequate systems and internal controls over customer data so as to ensure compliance with NBE Directives and other related rules and regulations.
c) Oversee the existence of appropriate risk management program and guidelines, and reporting processes in respect of the risk associated with the customer data privacy.
d) Oversee that relevant reports are sent by the Management to NBE without fail.
e) Delegate the Chief Executive Officer (CEO), as and when needed, for the management of customer data privacy activities in the Bank.
f) Review reports of the Management of the Bank and ensure that the Management takes timely actions on adverse reports.

2.2.2 Chief Executive Officer

The major roles and responsibilities of the CEO on the management of data privacy related activities are;

a) Oversee the overall management of customer data privacy related activities in the Bank. However, the CEO may delegate his/her authority to a concerned organ of the Bank or a Committee, as he/she may find it appropriate and necessary.
b) Approve operational procedure and guideline for the concerned organs of the Bank in relation to customer data privacy.
c) Oversee the proper implementation of the Data Privacy Policy and Procedure as well as NBE's directives in this regard and take remedial actions on deviations.
d) Review and send relevant reports to NBE, as required.
e) Review and send reports to the Board of Directors of the Bank, as required.

2.2.3 Director, Internal Audit

The major roles and responsibilities of the Director on the management of data privacy related activities are;

a) Ensure the existence of appropriate internal control systems related to ensuring customer data privacy.
b) Audit/inspect the activities related to customer data privacy and check the correctness of records, adherence to rules and regulations, and report its findings.
c) Follow-up that actions are taken to rectify errors, mistakes and any breach of the Bank's policy and procedure in relation to customer data privacy.
d) Prepare and submit to the Management and/or BODs, as appropriate, reports of audit findings.

SECTION THREE
DATA PRIVACY POLICY ITEMS

3.1 Collection of Data

3.1.1 The Bank shall collect customer's data;

a) Using lawful means,

b) For legitimate purposes necessary for the Bank's activities: to provide services, to communicate with the customer, and to make the Bank's services better, and

c) Others that are essential for its business.

3.1.2 The customer may be asked to provide the bank with certain personally identifiable information that can be used to contact or identify him/her ("Personal Data").

3.1.3 Personally Identifiable Information may include, but is not limited to: email address; first, second (father) and last (grandfather) name; company name, names of family members; phone numbers; address (include Woreda, sub-city, town/city, zone, and region), date of birth, income, etc.

3.1.4 The Bank shall collect personal data about a customer:

a) When the customer provides it to the Bank (e.g., where he/she contacts the bank via telephone, website, email or by any other means);

b) In the ordinary course of Bank's relationship with the customer (e.g., in the course of managing customer's transactions);

c) When the customer chooses to make public, including via social media (e.g., the bank may collect information from customer's social media profile(s), to the extent that he/she chooses to make his/her profile publicly visible);

d) When the customer visits the Bank's websites or uses any features or resources available on or through bank's website, his/her device and browser may automatically disclose certain information (such as device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to bank's website and other technical communications information), some of which may constitute Personal Data;

e) From third parties who provide it to the Bank (e.g., his/her employer; bank's customers; credit reference agencies; law enforcement authorities and so forth);

f) When the customer download, register or use bank's mobile applications.

3.1.5 The Bank may need to collect and process information on:

a) Potential parties that the Bank may deal with, such as potential customers, potential suppliers and third-party service providers, and potential candidates applying for a job at Bank, or any other party making a transaction with the Bank.

b) Parties associated with the Bank's customers or potential customers, such as their family members, customers, suppliers, etc.,

c) Parties related to Bank's employees or potential employees, such as their family members.

3.1.6 The Bank may be required by law to collect, record, use and store information in order to comply with the regulatory requirements.

3.1.7 The Bank will collect information from different available sources.

3.2 Data Storage

3.2.1 All data backup stored electronically on physical media shall be stored and secured in a locked box, drawer, cabinet, or similar equipment.

3.2.2 All data shall be stored and secured at the database.

3.2.3 Historical data shall be retained at the Bank's corporate data warehouse or at Bank's Disaster Recovery Center until the retention period elapsed and they are no longer required for on-going business operation of the Bank.

3.2.4 The data retention period shall be determined by the Bank's Top Management and the legal and regulatory requirements.

3.3 Use and Disclosure of Data

3.3.1 The Bank may only collect and use the information where the Bank has lawful grounds and legitimate business reasons to do so.

3.3.2 The customer shall authorize the Bank to exchange, share, part or all information related to the details and transaction history of the customer to its affiliates/ banks/ financial institutions/ credit bureaus/ agencies/ participation in any telecommunication or electronic clearing network as may be required by law, customary practice, credit reporting, statistical analysis and credit scoring, verification or risk management and shall not hold Awash Bank liable for use or disclosure of this information.

3.3.3 The Bank will use the collected information for the purpose it was gathered for and the Bank should have the customer's authorization prior to utilizing any of the collected data in case the Bank is planning to use it for something else.

3.3.4 The Bank shall be transparent in its dealings with the customer, and shall inform him/her about how it will collect and use the information. The Bank will use the information to:

a) Provide the customer with the products/services that the customer has requested;
b) Abide by the applied laws and regulations;
c) Protect the Bank's interest against any abuse or misuse of our services and products;
d) Carry out the customer's instructions;
e) Improve the Bank's products and services.

3.3.5 The Bank shall only use and disclose a financial customer's data for legitimate purposes agreed to it by the customer.

3.3.6 All relevant staff shall protect the Bank's proprietary information from unauthorized disclosure.

3.3.7 Employees shall not share data or information of the Bank informally.

3.3.8 Third parties shall have access to information only to perform tasks on behalf of the Bank and obligated not to disclose or use it for any other purpose without Bank's consent.

3.3.9 The Bank shall only use and disclose customer's data consistently with the original purpose of collection or with the explicit and informed consent of the customer.

3.3.10 The Bank may post the data security items on its Website or any other available means.

3.3.11 The Bank can disclose customer's data without their consent if requested by NBE, court or another relevant organ.

3.3.12 The Bank shall not be responsible for privacy practices of other websites other than the Bank's website.

3.4 Data Protection

3.4.1 The Bank shall keep its and customers' data confidential and secure.

3.4.2 All servers and computers containing data shall be protected by the monitoring system and the network and database firewall system.

3.4.3 To protect unauthorized activities on the data stores or database, the database application and servers shall be locked through strong password.

3.4.4 The relevant units of the Bank shall ensure that data is protected against misuse, unauthorized disclosure, accidental loss and destruction or damage.

3.4.5 Bank networks shall be adequately managed and controlled, in order to protect the data or information from potential threats such as information taping while the information is in transit.

3.4.6 Data flows between applications directly connected to servers or middleware layer shall be protected with a secure mechanism or encryption.

3.4.7 The communication between the Core Banking application and middleware application shall be protected with a secure mechanism or encryption.

3.4.8 All data of the Bank to be transferred physically, including that on removable electronic media, shall be transferred in a suitable strong container marked "confidential".

3.4.9 The Bank shall take reasonable steps to ensure that any third party to whom they disclose data keep them confidential and secure.

3.4.10 The Bank's data shall be encrypted before being transferred electronically.

3.4.11 Proper management approval shall be taken before moving any equipment from secured areas like Data Center.

3.4.12 Any staff shall not leave confidential documents on the desk; instead, it should be kept in a locked cabinet.

3.4.13 Any staff shall not leave customer related or confidential data printouts uncollected in the printer.

3.5 Data Access

3.5.1 Accessing data directly from data store shall not be allowed unless it is a must.

3.5.2 Based on the customers' request, unless it is prohibited by law, the Bank shall give them the right to access their data with a reasonable time.

3.5.3 Extracting data from the data store or database shall be officially requested by a Manager/Director or other similar supervisor and, shall be approved by the relevant Bank Organ.

3.5.4 Access to data shall be restricted only to those staff who need it for the Bank's business activities.

3.6 Data Retention and Disposal

3.6.1 Data, at the end of its retention period, shall be arranged and transferred to the location prepared for secure data disposal or destruction.

3.6.2 Data disposing team shall be established to apply an appropriate and strong oversight.

3.6.3 To avoid erroneous or unintended disposal, the data assumed no longer required for business operation and ended their retention period shall be thoroughly checked and further reviewed.

3.6.4 Strong monitoring and controlling system shall be established to ensure that the destruction has been completed as directed, particularly where the destruction is contracted out to an external service provider.

3.7 Customer's right

3.7.1 The Bank shall be obliged to protect the customers' personal data.

3.7.2 The Bank shall inform customers the type of personal data it is collecting and the purpose of collection.

3.8 Awareness, Training and Support

3.8.1 The Bank shall inform the customers how to protect their data, how to use it and avoid unnecessary disclosure of data.

3.8.2 The Bank shall inform the customers the kinds of data that it collects and the third parties to whom it may disclose such data.

3.8.3 Employees and Agents of AB shall be well trained to aware and give the required support to customers.

3.8.4 The Bank's website will contain links to other websites that may be of interest to its website visitors, such as; payment provider, advertising, LinkedIn, Facebook, you tube... etc.

3.8.5 The Bank will have to notify to all concerned that it is not responsible for the privacy practices of other websites.

3.8.6 The Bank will have to encourage customers to be aware and read the privacy statements of each website that it collects their personally identifiable information.

SECTION FOUR

ACCESS, EXCEPTIONS, REVISION, REPEAL, REPLACEMENT AND EFFECTIVE DATE

4.1 Access to this Policy

- This policy shall be kept in safe custody of the concerned supervisors in confidential manner.
- Access to this policy shall be limited only to the concerned organs/staff of the Bank that make use of the Policy for execution of their duties.

4.2 Exceptions to this Policy

- Any exceptional activities, decisions, and communications to this policy shall be forwarded to the BODs for approval prior to implementation.

4.3 Revision of this Policy

- Unless there is special enforcement to revise this policy in the meantime, it shall be revised every three years and approved by BODs.

4.4 Repeal and Replacement

- Any policies of the Bank contravening this policy and the existing data privacy policy are hereby repealed and replaced by this Data Privacy Policy.

4.5 Effective Date of this Policy

- This Data Privacy Policy shall be in force effective from _____ 2021.