Personal Data Privacy Position Statement

1. Our Commitment

Bank of Bahrain and Kuwait (herein referred to as “The Bank” or “BBK”) is committed to maintaining the confidentiality, integrity, and security of personal and sensitive information collected from customers, in accordance to applicable laws.

The Bank recognizes the importance of data privacy and manages data according to applicable data protection laws and regulations. This statement should be read in conjunction with any other privacy notices or fair processing notices and product terms and conditions that the Bank may provide on specific occasions when collecting or processing personal data.

2. Purpose & Scope

The purpose of this Position Statement is to provide the Bank with a transparent approach towards managing the personal information of BBK customers. This approach includes using measures to manage information risks, directives for the protection of information assets across of business units, providing Bank employees with access to all Bank policies and ethical guidelines, and providing ongoing employee training to reinforce their understanding and implementation of data privacy and security measures.

The scope of this Position Statement includes the information stored, communicated, deleted, and processed within the Bank on all media and system platforms through any communication channel.

This Position Statement is supported by the Bank’s senior magagement.

3. Data Collection

The Bank collects and uses information about its customers to provide them with high-quality financial products and services. The kind of information BBK collects from customers includes:

Data class	Indicative data elements
Individual’s information	Name, Phone Number, Residential Address, CPR Number, Passport Number, Email Address, Date of Birth, Employment Information, Salary Information, Credit Information
Legal entity’s information	Name, Commercial Registration Number, Registered Address, VAT Registration Number, and information concerning shareholders, management and credit
Financial information of legal entities	Turnover (Sales), Net Profit, Net Worth (Total Assets, Total Liabilities)
Transaction information	Banking Transactions (Recipients, Transaction Amounts, Corresponding Bank, Destination Country)
Website and application usage information	Time Spent, Pages Visited
Cookies, log files and web beacons	IP Address, Device Identifiers

4. Data Protection

BBK safeguards the privacy of personal information through adequate security measures as appropriate to the sensitivity of the information. The collected personal information will be used for authorized purposes and will not be processed for other purposes.

As part of the Bank's efforts to maintain data privacy and security, significant technical and administrative security measures are used to protect any information from loss, misuse, unauthorized access, and disclosure. The following measures are to be followed:

- Deploying security controls such as identity authentication, regular network risk assessment and updates, stringent monitoring and detection systems.
- Adopting ISO 27001 certification for information security management and PCI-DSS.
- Reporting on data breaches through annual reporting.
- Conducting regular cyber security stress tests to measure performance.
- Periodically carrying out internal and external audits on data processing systems.
- Implementing new solutions in cybersecurity and exploring new technologies related to Artificial Intellegience (AI) and FinTech.
- Providing regular training and awareness initiatives for all employees to guarantee a culture of compliance to internal privacy and security regulation.
- Employing a cyber security executive or establishing an Information Security Committee.
- Conducting reviews to this Position Statement and related procedures and standards at least annually or when significant changes to the Bank and/or its environment occurs, assuringits continuing suitability, adequacy, and effectiveness.
- Ensuring that processed data is only shared with authorized users and systems to prevent data misuse. Shared data (both internally and externally) shall not have any linkage to the Bank's customers' personal identity.