Privacy Policy

Introduction:

At Cairo Amman Bank and all its affiliated brands (CAB/Signature/LINC), we are fully committed to protecting the privacy and security of your personal data in accordance with the provisions of the Personal Data Protection Law No. (24) of 2023 and the instructions of the Central Bank of Jordan. This Privacy Policy explains how your personal data is collected, used, disclosed, and processed in general, as well as the measures adopted to protect it when we provide our services to you directly, when you visit our website, when you use our digital services online, or during any other electronic interaction with the Bank or its affiliated brands.

Objectives of the Privacy Policy

This Privacy Policy aims to protect the personal data of individuals who are customers of the Bank or deal with it, and to ensure the confidentiality of information and its secure processing in accordance with applicable laws and regulations. It also seeks to achieve transparency in the collection and use of data, enable individuals to exercise their legal rights, and define the legitimate purposes for processing personal data in a manner that ensures the efficient provision of banking services, compliance with regulatory requirements, and the enhancement of trust and credibility between the Bank and its customers through the application of the highest security standards and technical measures to protect information.

1. Information We Collect

We collect various types of information to provide and improve our services, manage our relationship with you, and comply with legal obligations. This information may include the following:

1.1. Personal Data You Provide Directly:

Information you provide to us when applying for a product or service, registering for mobile banking services, contacting customer service, or interacting with us through forms on our website. This may include, for example:

- **Identity data:** name, date of birth, national number, passport number, nationality, gender.
- **Contact information:** address, email address, phone number.
- **Financial information:** account numbers, income, credit history.
- Other data: information you provide through surveys, feedback, or customer service interactions.

1.2. Data Collected Indirectly:

We may obtain personal data about you indirectly from various sources:

- **Automatically:** Our website uses cookies and similar tracking technologies to enhance your browsing experience, analyze website traffic, and personalize content and advertisements. You can manage your cookie preferences through your browser settings or through our website's cookie consent tool when visiting our website. This may include, for example:
  - **Device information:** Internet Protocol (IP) address, device type, operating system, browser type.
  - **Usage data:** pages visited, time spent on pages, links clicked, referring URLs, interaction patterns.
  - **Location data:** general geographic location based on IP address.

1.3. Information from Third Parties:

We may receive information about you from third parties, such as credit inquiries and identity verification services, or related or connected parties such as your legal representative, agent, authorized signatory, or employer.

1.4. From Publicly Available Sources:

Such as public databases and the Companies Control Department website, in accordance with applicable laws.

2. How We Use Your Information (Purposes and Legal Basis)

We use your personal data for various purposes:

- Providing banking services and processing transactions (contractual necessity)
- Verifying your identity and ensuring account security (contractual necessity)
- Communicating with you regarding your accounts and our services (contractual necessity / legitimate interest)
- Improving our products and services and enhancing your experience (legitimate interest)
- Complying with legal and regulatory requirements (legal basis)
- Detecting and preventing financial crimes, fraud, and money laundering (legal basis)
- Conducting data analysis, research, and internal administrative purposes (legitimate interest).

The following matrix illustrates how personal data is used:

Type of Data	Purpose of Processing	Legal Basis
Personal identity details (name, date of birth, email address, nationality, marital status, gender, contact information)	Account management, communication, provision of banking services, compliance with regulatory requirements	Cases permitted by law, performance of contracts, legal and regulatory obligation
Health data (physical, psychological, genetic)	Providing special services when required, compliance with legal requirements	Cases permitted by law, legal and regulatory obligation
Addresses and supporting proof documents	Account management, compliance with regulatory requirements	Legal and regulatory obligation, performance of contracts
Identity verification documents (ID card, passport)	Identity verification, compliance with regulatory requirements, and anti money laundering	Legal and regulatory obligation
Employment and employer data	Loan application assessment, account management, compliance with regulatory requirements	Cases permitted by law, performance of contracts, legal and regulatory obligation
Financial details (income, source of wealth, financial activity)	Account management, risk assessment, compliance with regulatory requirements	Legal and regulatory obligation, legitimate interest
Tax status data (Tax Identification Number, FATCA)	Compliance with international tax requirements	Legal and regulatory obligation
Financial transaction details	Account management, fraud prevention, compliance with regulatory requirements	Legal and regulatory obligation
Digital identifiers (IP address, email address)	Cybersecurity, provision of electronic services	Legitimate interest, legal obligation
Geolocation data and use of ATMs and branches	Service improvement, fraud prevention	Legitimate interest, legal obligation
Cookies	Enhancing user experience, electronic services	Explicit consent, cases permitted by law
Audio, visual, and photographic data, including images captured by surveillance cameras	Security, identity verification	Legal obligation, legitimate interest
Risk classification information	Credit assessment, risk management	Legitimate interest
Due diligence data	Compliance with regulatory requirements	Legal and regulatory obligation, cases permitted by law
Data of individuals related to you	Account management, compliance with regulatory requirements	Explicit consent, legal obligation

3. Mobile Banking Services

Our mobile banking services are designed to provide secure and convenient access to your accounts. When you use our mobile application, we collect specific data to enhance security and user experience, which may include:

- **Device information:** We collect information about your mobile device, such as model, operating system, and unique device identifiers to authenticate your device and protect your account.
- **Geolocation:** We may use your device's location to provide location based services and for fraud prevention purposes.
- **Biometric data:** Subject to your explicit consent, which will be obtained separately through the mobile application interface, we may use biometric authentication (such as fingerprint or facial recognition) to log in and conduct transactions securely.

4. Cookies and Tracking Technologies

Our website uses cookies and similar tracking technologies to enhance your browsing experience, analyze website traffic, and personalize content and advertisements. You can manage your cookie preferences through your browser settings or our website's cookie consent tool.

5. How We Share Your Information

We may share your personal data with third parties only when necessary and for the purposes outlined in this Policy, in compliance with legal requirements. Such parties may include:

- **Service providers:** Intermediaries involved in executing financial, banking, and exchange operations, including correspondent banks and licensed or approved electronic payment and money transfer companies, where data is shared and processed to the extent necessary to execute such operations and comply with legislative and regulatory requirements.
- **Regulatory and legal authorities:** Government bodies and supervisory authorities (such as the Central Bank of Jordan and the Anti Money Laundering Unit), and courts, when required by law or upon a legitimate request.
- **Credit reporting agencies:** For credit assessment and reporting purposes, as permitted by law.
- **Professional advisors:** Auditors and lawyers for audit, compliance, and legal representation purposes.

6. International Data Transfers

Your personal data may be transferred to countries outside the Hashemite Kingdom of Jordan under the following conditions:

- The existence of a legal basis for the transfer, such as the necessity to perform a contract with the data subject (e.g., fund transfers), prior consent, or compliance with legal obligations imposed by legislation.
- The existence of a justification for transferring data outside the Kingdom as required by the nature of the Bank's business, such as regional operations outside the Kingdom or the nature of the transaction or service.
- The availability of appropriate security safeguards to protect your privacy rights in accordance with the Jordanian Personal Data Protection Law of 2023.

7. Data Security

Cairo Amman Bank is committed to protecting the privacy of your data. Our policies include a comprehensive set of technical, physical, and organizational measures designed to maintain the integrity and confidentiality of your data. These measures protect your data from loss, misuse, unauthorized access, data breaches, or alteration during storage, processing, or transmission. We continuously evaluate and update our security measures to ensure ongoing protection. Access to your personal data is restricted to authorized employees who need it to provide Cairo Amman Bank services or products.

8. Data Retention

The Bank is committed to retaining your personal data only for the period necessary to achieve the purposes for which it was collected, as well as to comply with legal, regulatory, and statutory obligations, in accordance with the instructions of the Central Bank of Jordan (CBJ) and other applicable laws. These may require the Bank to retain certain customer information for a period of no less than ten (10) years after the termination of the banking relationship, unless a longer period is required by law.

Your personal data will be securely disposed of once it is no longer needed.

9. Your Rights (Data Subject Rights)

Pursuant to the Jordanian Personal Data Protection Law and the instructions of the Central Bank of Jordan, the Bank may process personal data without the consent or notification of the data subject for the purpose of enabling the Bank to carry out its licensed activities. Otherwise, you have certain rights in relation to your personal data, including:

- **Right of access:** Request a copy of the personal data we hold about you.
- **Right to rectification:** Request correction of inaccurate or incomplete personal data.
- **Right to erasure (right to be forgotten):** Request deletion of your personal data under certain conditions and in accordance with CBJ instructions and applicable laws in the Hashemite Kingdom of Jordan, provided that the processing is not for the Bank's legitimate purposes.
- **Right to restrict processing:** Request restriction of how we use your personal data, by suspending or limiting its use for a certain period, provided that the processing is not for the Bank's legitimate purposes.
- **Right to object to processing:** Object to the processing of your personal data under certain conditions (such as for direct marketing purposes).
- **Right to data portability:** Request to receive your personal data in a structured, commonly used, and machine-readable format, and enable you to use it or transfer it to another party.
- **Right to withdraw consent:** You have the right to withdraw your consent at any time, provided that the processing is not for the Bank's legitimate purposes.

  It is emphasized that the Bank may not be able to respond to requests that conflict with applicable legislation or regulatory and supervisory requirements, or that may result in the concealment, alteration, or intentional modification of information necessary to identify the customer and the beneficial owner, the accuracy of credit reports, due diligence requirements, or that conflict with the security and safety of the Bank's operations or expose them to risk.

Data Processing: One or more operations carried out by any means or method for the purpose of collecting, recording, copying, preserving, storing, organizing, refining, exploiting, using, sending, distributing, publishing, linking with other data, making available, transferring, displaying, anonymizing, encoding, destroying, restricting, erasing, modifying, describing, or disclosing data by any means whatsoever.

10. Mechanisms for Submitting Requests and Complaints

To exercise any of these rights or to submit a complaint, please contact our Data Protection Officer (DPO) through the channels listed below. We will handle and respond to all requests and complaints as follows:

- **Personal data related requests:** Implemented within 15 days from the day following receipt of the request. The Bank may extend this period once for a similar duration.
- **Complaints:** Responded to within 10 days from the day following receipt of the complaint.

  Note: We may not be able to fulfill certain requests if they conflict with legal or regulatory requirements or if they pose a risk to the security of our operations.

11. Notification of Data Breach

In the event of a personal data breach, the data subject will be notified within 24 hours if the breach is likely to pose a significant risk to the rights and freedoms of the individual.

12. Marketing Provisions
The Bank uses customer data for the purpose of directly marketing the Bank's services and products, within the scope of the services and products provided to the customer under the relationship between the customer and the Bank. This includes similar or related services and products, including those offered by companies wholly owned by the Bank. The customer has the right to unsubscribe from direct marketing channels during the first communication.

13. Changes to the Privacy Policy
We update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. We will notify you of any material changes by publishing the updated policy on our website with a new effective date. We encourage you to review this Policy periodically.

14. Contact Us
If you have any questions about this Privacy Policy, our data practices, or if you wish to exercise your rights, please contact our Data Protection Officer (DPO) at:
Cairo Amman Bank
Personal Data Protection Officer: Ahmed Khleifat
Email: DPO@cab.jo
Phone: 065007700