Supplemental Provisions - Jordan

Requirements under Jordan Personal Data Protection Law (Law No. 24 of 2023) and the applicable Implementation regulations

This supplemental provision for Jordan (Jordan supplement) compliments the global privacy notice/Policy for institutional clients (the Global privacy notices) and applies to individuals who have the rights under the law number 24 of 2023 and the implementation regulations in connection with the processing of personal data and sensitive personal data (Personal Data) by our markets, services, banking operations in Jordan.

Citibank, N.A., Jordan (Citi Jordan) provides products and services to enterprises (Corporations), Financial Institutions, public sector organizations. Processing of Personal data from Citi Jordan that involves Personal Data or would require an international data transfer to other Citigroup affiliates for onward processing (that shall be identical or directly related to the purposes of the initial data collection) and in line with the Central Bank of Jordan regulations.

Specific Terms:

Article 6-8 Pursuant to the Law No. (24) of the year 2023 Personal Data Protection Law "**PDPL**" or **Law**" along with the relevant implementation regulations issued from the Central bank of Jordan as well the Ministry of Digital Economy as applicable; please find below the relevant definitions.

- **Key Definitions**

Personal Data	:	Any data or information that pertain to a natural person and that is capable of identifying him/ her whether directly or indirectly notwithstanding the source or form thereof, including the data that relate to the personality, family status, or places of existence of such person.
Sensitive Personal Data	:	Any data or information that pertain to a natural person and which indicates for that person (whether directly or indirectly), the origin or ethnicity, the political opinions or affiliations, or the religious beliefs, as well as any data that relates to the financial position; health, physical, mental, or genetic status, biometrical measures, or the criminal record thereof, or any information or data the Board/Executive Management for branches resolves to consider sensitive if the disclosure or misuse of the same will lead to harm to such Data's Subject Person
Data	:	Personal Data and Sensitive Personal Data.
Data Bases	:	Electronic or non-electronic files or records that contain Data.

Processing	:	One operation or more, made in any form or means with the view of collecting, recording, copying, saving, storing, organising, refining, exploiting, using, sending, distributing, or publishing Data, or linking such Data to other data, or otherwise making available, transferring, presenting, pseudonymising, hiding the coding of, or destroying such Data.
The responsible Person	:	Any natural or juridical person, whether inside or outside the Kingdom, under whose possession are Personal Data
The Processor	:	The natural or juridical person who is in charge of Data Processing.
The Controller	:	The natural person appointed to supervise Data Bases and Processing in accordance with the provisions of this Law.
The Recipient	:	Any natural or juridical person, whether inside or outside the Kingdom, to whom the Data is transferred or with whom the Data is exchanged by the Responsible Officer.

Lawful Basis Requirements

Processing may be considered lawful and permissible without the data subject's valid consent **i**n the following cases as per CBJ Decision:

1. Where it is required or authorized under legislation, for the implementation thereof, or pursuant to a decision issued by a competent judicial authority.
2. Compliance with the legal requirements under the applicable Anti-Money Laundering and Counter-Terrorist Financing Law and the regulations and instructions issued pursuant thereto, including for the purposes of screening against sanction and prohibition lists issued pursuant to United Nations Security Council resolutions, and responding to requests and instructions from the competent regulatory authorities legally authorized to do so, as well as from law enforcement authorities.
3. Where the processing is necessary to comply with supervisory requirements issued by the competent authorities legally authorized to do so, including requirements issued by such authorities to protect the stability of the financial system or the public interest.
4. Where the processing is necessary for the Bank to take the necessary measures to combat financial fraud, or for the implementation of procedures issued by the competent authorities legally authorized to do so.
5. Where the processing is necessary for the Bank to verify the integrity, accuracy, and security of the operations it carries out.
6. For the purposes of the Bank carrying out anonymization or pseudonymization instructions.

7. For the purposes of the Bank undertaking the necessary measures for cybersecurity, its operations, and services, including testing procedures related to cyberattacks and analyzing data traffic across networks to detect threats and suspicious activities.
8. Verifying the personal data provided by the customer regarding the Bank of individuals who do not have a direct relationship with the Bank, such as the beneficiary of the customer relationship or transaction, the guarantor, agent, guardian, legal representative, shareholders, partners, directors, representatives, authorized signatories, and employees of customers that are legal entities, as well as family members, general/special successors, rights holders, reference contacts, and the details of persons who may be contacted in case of emergency.
9. Where the processing is necessary and related to the execution of the activities, services, and products provided by the Bank to the data subject, or to similar or related operations, or for the performance of a contract between the Bank and the data subject.
10. Where the processing is necessary for the purposes of reinsurance arrangements.
11. To serve a necessary interest of the data subject or to protect their vital interests, where it is not possible or is difficult to contact them, provided that the Bank can provide evidence of the existence of such interest and the impossibility or difficulty of contacting the data subject.

Purpose of Processing:

We process your personal data inside or outside Jordan , as necessary to pursue our legitimate business and other interests, for the following reasons:

- To provide financial products and services to our clients and to communicate with you and/or our clients about them.
- To manage, administer and improve our business and client and service provider engagements and relationships and for corporate marketing, business development and analysis purposes.
- To monitor and analyze the use of our products and services for system administration, operation, testing and support purposes.
- To operate and manage our information technology and systems, and to ensure the security of our information technology and systems.
- To establish, exercise and/or defend legal claims or rights and to protect, exercise and enforce our rights, property, or safety, or to assist our clients or others to do this; and
- To investigate, respond to and address complaints or incidents relating to us or our business, to maintain service quality and to train our staff.

We also process your personal data to comply with laws and regulations. We sometimes do more than the minimum necessary to comply with those laws and regulations, but only as necessary to pursue our legitimate interests in cooperating with our regulators and other authorities, preventing, or detecting financial and other crimes and regulatory breaches, and protecting our businesses and the integrity of the financial markets. This involves processing your personal data for the following reasons:

- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies, financial markets or other intermediaries or counterparties, courts or other third parties to the extent permitted by law.

- to monitor and analyse the use of our products and services for risk assessment and control purposes, including detection, prevention, and investigation of fraud.
- to conduct compliance activities such as audit and reporting, assessing, and managing risk, maintenance of accounting and tax records, fraud, and anti-money laundering (AML) prevention and measures relating to sanctions and antiterrorism laws and regulations and fighting crime. This includes know your customer (KYC) screening (which involves identity checks and verifying address and contact details), politically exposed persons screening (Which involves screening client records against internal and external databases to establish).

Provisions related to Marketing To exercise your statutory rights to inhibit direct marketing from Citi Jordan or to be subject to commercial profiling as set out in the PDPL, you may:

- Where you are an end-user of Citi's global platforms like (Citidirect, CitiVelocity etc..) use communication and marketing preferences in the user menu that enable and disable contacting and marketing options.
- At the bottom of electronic marketing communications, click on the "unsubscribe" option on the footer.
- In our website , opt-in (and opt out) of cookie selections or "do not share my data" as the case may be.
- Or directly writing to Citi Jordan, on the below detail contact mentioned below.
  any

Records of Processing Activities

1) (a) The Bank shall maintain a record of data processing activities for the entire duration of such processing and retain the record for **any periods required by the applicable legislation**, provided that it shall be no less than five years starting from the date the processing ends. Accordingly, Citi Jordan shall continue to follow its retention schedule and records management policies and procedures as well its retention schedule according

(

Linked here to access the further regulations from the Ministry of Digital Economy in Jordan which include but not limited the guidelines regarding the security of the Data , DPIA and the severity of an information security accident / the required assessment and on whether the incident should be reported or not (consult with Country legal & ICRM) along with relevant forms to be used for any reporting.

Right in Relation with Personal Data Processing

You may ask us to: (i) provide you with a copy of your personal data; (ii) correct your personal data; (iii) erase your personal data: or (iv) restrict our processing of your personal data. You may also object to our processing of your personal data. These rights will be restricted or limited in some situations, in accordance with applicable Jordanian laws & regulations including: (a) the Personal Data Protection Law as well Central Bank of Jordan the applicable regulations or (b) for the bank's Security purposes of the entity (e.g., CCTV surveillance or video monitoring) or (c)that may result in the concealment, alteration, or deliberate modification of information necessary to identify the customer and the beneficial owner or to verify the accuracy of their credit report, or that may affect due diligence requirements, or conflict with the security and integrity of the operations carried out by the bank or expose them to risk.

To exercise these rights or if you have questions about how we process your personal data, please contact us using the contact details in this notice. You may also complain to the relevant data protection authorities in Jordan. You can find contact information for the Jordan Personal Data Protection Council here (Jordan PDPL):

Contact information and Complaints

In the event you wish to contact us or raise a complaint – please reach out to the following contact details:

Email Contact: jordan.dataprivacy@citi.com

Address: Citibank N.A – Prince Shaker Bin Zeid Street Building 29, Shmeisani, Amman - Jordan

Web address: **https://www.citibank.com/icg/sa/emea/jordan/local-contact.html**