Confidentiality and Data Privacy Conditions

1. Introduction.

These conditions ("**Conditions**") explain how each party may use, and must protect, the other party's Confidential Information (including Personal Data) in connection with the provision by the Bank, and receipt and use by the Customer, of accounts and other products and services, whether or not account-related (collectively, "**Services**"). "**Bank**" has the meaning specified in the terms and conditions which incorporate or otherwise reference these Conditions.

2. Protection of Confidential Information.

2.1 Definitions.

"Confidential Information" means information (in tangible or intangible form) relating to the disclosing party and/or its affiliates (including any entity that directly or indirectly controls, is controlled by or is under common control with, a party), branches or representative offices (collectively, **"Affiliates"**) or their respective Representatives or Owners, that is received or accessed by the receiving party or its Affiliates or their respective Representatives in connection with providing, receiving or using Services. "Confidential Information" includes Personal Data, information relating to the Bank's products and services and the terms and conditions on which they are provided, technology (including software, the form and format of reports and online computer screens), pricing information, internal policies, operational procedures, bank account details, transactional information, and any other information, in each case that: (i) is designated by the disclosing party as confidential at the time of disclosure; (ii) is protected by applicable bank secrecy or other laws and regulations; or (iii) a reasonable person would consider to be of a confidential and/or proprietary nature given the nature of the information and the circumstances of its disclosure.

"Owner" means any natural person or entity (or its branch) that: (i) owns, directly or indirectly, stock of, or profits, interests or capital or beneficial interests in, a party; or (ii) otherwise owns or exercises control over a party directly or indirectly through ownership, controlling interest or any other arrangement or means, including: (a) a person who ultimately has a controlling interest in, or who otherwise exercises control over, a party; or (b) the senior managing official(s) of a party.

"Representatives" means a party's officers, directors, employees, contractors, agents, representatives, professional advisers and Third Party Service Providers.

2.2 Protection.

The receiving party will keep the disclosing party's Confidential Information confidential on the terms hereof and exercise at least the same degree of care with respect to the disclosing party's Confidential Information that the receiving party exercises to protect its own Confidential Information of a similar nature, and in any event, no less than reasonable care. The receiving party will only use and disclose the disclosing party's Confidential Information to the extent permitted in these Conditions.

2.3 Exceptions to Confidentiality.

Notwithstanding anything in these Conditions to the contrary but subject to Data Protection Law, the restrictions on the use and disclosure of Confidential Information in these Conditions do not apply to information that: (i) is in or enters the public domain other than as a result of the wrongful act or omission of the receiving party or its Affiliates or their respective Representatives in breach of these Conditions; (ii) is lawfully obtained by the receiving party from a third party, or is already known by the receiving party, in each case without notice of any obligation to maintain it as confidential; (iii) is independently developed by the receiving party without reference to the disclosing party's Confidential Information; (iv) an authorized officer of the disclosing party has agreed in writing that the receiving party may disclose on a non-confidential basis; or (v) has been anonymized and/or aggregated with other information such that neither the Confidential Information of the disclosing party nor the identity of any Data Subject is disclosed.

3. Authorized Disclosures.

3.1 Definitions.

"Bank Recipients" means the Bank, Bank Affiliates and their respective Representatives.

"Payment Facilitator" means a third party that forms part of a payment system infrastructure or which otherwise facilitates payments, including without limitation: communications, clearing and other payment systems or similar service providers; intermediary, agent and correspondent banks; digital or ewallets; or similar entities.

"Permitted Purposes" means in relation to a party's (or its Affiliates' or their respective Representatives') use of the other party's (or its Affiliates' or their respective Representatives') Confidential Information:

(A) To provide, or to receive and use, the Services in accordance with their respective terms and conditions and to undertake related activities, such as, by way of non-exhaustive example:

(1) To fulfill applicable domestic and foreign legal, regulatory and compliance requirements (including know your customer (KYC) and anti-money laundering (AML) obligations applicable to a party and/or its Affiliates) and to otherwise make the disclosures specified in Condition 3.3 (Legal and regulatory disclosure);

(2) To verify the identity or authority of a party's Representatives who interact with the other party;

(3) For risk assessment, information security management, statistical, trend analysis and planning purposes;

(4) To monitor and record calls and electronic communications with the other party for quality, training, investigation and fraud and other crime prevention purposes;

(5) For fraud and other crime detection, prevention, investigation and prosecution;

(6) To enforce and defend a party's or its Affiliates' rights; and

(7) To manage a party's relationship with the other party (which may include the Bank providing information to the Customer and its Affiliates about the Bank's and Bank Affiliates' products and services);

(B) To make disclosures to third parties to whose accounts the Customer instructs the Bank or Bank Affiliates to make or receive a payment from an account, or to enable such third parties to perform payment reconciliations;

(C) To make disclosures to Payment Facilitators and to the Bank's and Bank Affiliates' Third Party Service Providers in connection with the provision of the Services;

(D) To make disclosures to, and to obtain information from, credit information bureaus, credit rating agencies, central banks or other bodies in connection with risk-based analysis and decisions by the Bank or where such disclosures are otherwise required by applicable law or regulation;

(E) To make disclosures to the disclosing party's Affiliates and third party designees;

(F) In connection with the provision of products and services (including supporting the opening of accounts) by the Bank and Bank Affiliates to the Customer's Affiliates; and

(G) For any additional purposes expressly authorized by the other party.

"Third Party Service Provider" means a third party selected by the receiving party or its Affiliate to provide services to or for the benefit of the receiving party, and who is not a Payment Facilitator (eg, technology service providers, business process service providers, call center service providers, outsourcing service providers, consultants and other external advisors).

3.2 Permitted Disclosures.

The disclosing party agrees (and where required by applicable bank secrecy or other laws is hereby deemed to provide a waiver and/or release to ensure) that the receiving party may use and disclose the disclosing party's Confidential Information to the receiving party's Affiliates and to its and their respective Representatives, Payment Facilitators and any other third party recipients specified in these Conditions, who require access to such Confidential Information to the extent reasonably necessary to fulfil the relevant Permitted Purposes. The receiving party shall ensure that any of its Affiliates and Representatives to whom the disclosing party's Confidential Information is disclosed pursuant to this Condition 3.2 shall be bound to keep such Confidential Information confidential and to use it for only the relevant Permitted Purposes.

3.3 Legal and Regulatory Disclosures.

The disclosing party agrees (and where required by applicable bank secrecy or other laws is hereby deemed to provide a waiver and/or release to ensure) that the receiving party (and, where the Bank is the receiving party, Bank Recipients and Payment Facilitators) may disclose the disclosing party's Confidential Information pursuant to: (i) legal process; (ii) any other domestic or foreign legal and/or regulatory permission, obligation or request; (iii) agreement entered into by any of them and any domestic or foreign governmental authority; or (iv) between or among any two or more domestic or foreign governmental authorities, including disclosure to courts, tribunals, and/or legal, regulatory, tax and other governmental authorities.

4. Retention Period.

Each of the Customer and Bank Recipients may retain, use, and as applicable Process, the other party's Confidential Information for the period of time reasonably necessary for the relevant Permitted Purposes. On termination of the provision of the Services (including closure of accounts), each of the Customer and Bank Recipients shall be entitled to retain, use, and as applicable Process, the other party's Confidential Information for legal, regulatory, audit and internal compliance purposes and in accordance with their internal records management policies, to the extent that this is permissible under applicable laws and regulations, and otherwise in accordance with these Conditions, but shall otherwise securely destroy or delete such Confidential Information.

5. Information Security.

The Bank will, and will use reasonable endeavors to ensure that Bank Affiliates and Third Party Service Providers will, implement reasonable and appropriate physical, technical and organizational security measures to protect Customer Confidential Information that is within its or their custody or control against unauthorized or unlawful use (or in the case of Personal Data, unlawful Processing) and accidental destruction or loss.

6. Personal Data.

6.1 Definitions.

"Data Protection Law" means any and all applicable data protection and privacy laws and regulations relating to the Processing of Personal Data, including any amendments or supplements to or replacements thereof.

"Data Subject" means a natural person who is identified, or who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity, or, if different, the meaning given to this term or nearest equivalent term under Data Protection Law.

"Personal Data" means any information that can be used, directly or indirectly, alone or in combination with other information, to identify a Data Subject, or if different, the meaning given to this term or nearest equivalent term under Data Protection Law.

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, or, if different, the meaning given to this term or nearest equivalent term under Data Protection Law.

"Security Incident" means an incident whereby the confidentiality of disclosing party Personal Data within the receiving party's custody or control has been materially compromised in violation of these Conditions so as to pose a reasonable likelihood of harm to the Data Subjects involved.

6.2 Compliance with Data Protection Law.

In connection with the provision or receipt and use of the Services: (i) each party will comply with Data Protection Law; and (ii) the Customer confirms that any Personal Data that it provides to Bank Recipients has been Processed fairly and lawfully, is accurate and is relevant for the purposes for which it is being provided.

6.3 Cross-border Personal Data Transfers.

The Customer acknowledges, and where required by applicable law or regulation agrees, that in the connection with providing the Services and otherwise making disclosures pursuant to Condition 3 (Authorized Disclosures), Personal Data of Customer Data Subjects (eg, the Customer's or its Affiliates' respective Representatives and Owners) may be disclosed and/or transferred to recipients located in countries other than the country in which the Bank entity or its branch which provides the Services is established or the Customer is located. However, the Bank: (i) requires its Affiliates and Third Party Service Providers to protect Personal Data pursuant to Condition 5 (Information Security); and (ii) carries out cross-border transfers of Personal Data in accordance with Data Protection Law.

6.4 Legal Basis for Processing Personal Data.

To the extent that the Bank Processes Personal Data of Customer Data Subjects, the Customer warrants that it has, if and to the extent required by Data Protection Law, provided notice to and obtained valid consent from such Data Subjects in relation to the Bank's Processing of their Personal Data as described in these Conditions, and in any applicable Bank Privacy Statement or other privacy disclosure(s) accessible at https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (or such other URL or statement as the Bank may notify to the Customer from time to time). If the Customer is itself a Data Subject, the Customer warrants that if and to the extent required by Data Protection Law: (a) it has received the privacy disclosure(s) referenced in the preceding sentence; and (b) it consents to such Processing.

6.5 Security Incidents

(A) If the Bank becomes aware of a Security Incident, the Bank will investigate and remediate the effects of the Security Incident in accordance with its internal policies and procedures and the requirements of applicable laws and regulations. The Bank will notify the Customer of a Security Incident as soon as reasonably practicable after the Bank becomes aware of it, unless the Bank is subject to a legal or regulatory constraint, or if it would compromise the Bank's investigation.

(B) Each party is responsible for making any notifications to regulators and Data Subjects concerning a Security Incident that it is required to make under Data Protection Law. Each party will provide reasonable information and assistance to the other party to the extent necessary to help the other party to meet its obligations to regulators and Data Subjects.

(C) Neither party will issue press or media statements or comments in connection with any Security Incident that name the other party unless it has obtained the other party's prior written permission.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

© 2020 Citibank, N.A. All rights reserved. Citi and Citi and Arc Design are trademarks and service marks of Citigroup Inc. or its affiliates and are used and registered throughout the world.
1977432 06/20