

Confidentiality and Data Privacy Conditions

Podmienky mlčanlivosti a ochrany dôvernosti údajov

1. Introduction

These Conditions form part of the terms and conditions that apply between the Customer and the Bank in relation to the provision of Accounts and Services to the Customer. For the purpose of these Conditions, "Services" shall also include any services, transactions or dealings between the Bank and the Customer, whether or not related to the Customer's Account; these Conditions shall be in addition to any other terms and conditions agreed to between the Bank and the Customer. These Conditions set out each party's obligations in relation to Confidential Information and Personal Data received from the other party in connection with the provision of Accounts and Services. Some provisions of these Conditions are region-specific and will only apply in respect of the regions or countries specified. In some countries, further country-specific terms are required, and these will be included in the Local Conditions and/or Regulatory Disclosures, Declarations and Representations (RDDR) for that country. Except to the extent prohibited under applicable law or expressly agreed otherwise by the parties, and subject to any mandatory minimum notice period prescribed by applicable law, these Conditions may be updated from time to time with general applicability to customers upon written notice to the Customer. If there is a conflict between these Conditions and any agreement between the Bank and the Customer related to any Bank product or Service, the agreement related to the Bank product or Service prevails to the extent of any such conflict.

2. Protection of Confidential Information

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.

3. Use and disclosure of Confidential Information

The Disclosing Party hereby grants the Receiving Party the right to use and disclose the Disclosing Party's Confidential Information to the extent necessary to accomplish the relevant Permitted Purposes. The Receiving Party will only use and disclose the Disclosing Party's Confidential Information to the extent permitted in these Conditions.

4. Exceptions to confidentiality

Notwithstanding anything in these Conditions to the contrary, 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

1. Úvod

Tieto Podmienky mlčanlivosti a ochrany dôvernosti údajov (CDPC) sú nedeliteľnou súčasťou podmienok, ktoré sa uplatňujú medzi Klientom a Bankou v súvislosti s vedením Účtov a poskytovaním Služieb Klientovi. Pre účely týchto CDPC, „Služby“ budú tiež zahŕňať akékoľvek služby, transakcie alebo obchody medzi Bankou a Klientom, bez ohľadu na to, či sa týkajú Účtu Klienta alebo nie; tieto CDPC dopĺňajú akékoľvek iné obchodné podmienky uzavreté medzi Bankou a Klientom. Tieto CDPC stanovujú všetky práva a povinnosti zmluvných strán týkajúce sa Dôverných informácií a Osobných údajov získaných od druhej strany vo vzťahu k vedeniu Účtov a poskytovaniu Služieb. Niektoré ustanovenia týchto CDPC sú pre každý región špecifické a budú sa aplikovať iba na uvedené regióny a krajiny. V niektorých krajinách sa vyžadujú ďalšie podmienky špecifické pre danú krajinu, ktoré budú zahrnuté v Miestnych podmienkach pre danú krajinu a/alebo v Právnych oznámeniach a vyhláseniach („RDDR“) pre danú krajinu. S výnimkou prípadov kedy to zakazujú príslušné právne predpisy, alebo ak je to výslovné dohodnuté inak medzi zmluvnými stranami a za podmienky splnenia akékoľvek minimálnej povinnej lehoty na predchádzajúce oznámenie, tieto CDPC môžu byť aktualizované z času na čas so všeobecnou platnosťou pre všetkých klientov na základe písomného oznámenia Klientovi. V prípade rozporu medzi ustanoveniami týchto CDPC a ustanoveniami akékoľvek dohody medzi Bankou a Klientom týkajúcej sa akéhokoľvek produktu alebo Služby Banky, bude mať prednosť takáto dohoda týkajúca sa produktu alebo Služby Banky.

2. Ochrana Dôverných informácií

Prijímajúca strana bude uchovávať Dôverné informácie Poskytujúcej strany ako dôverné v súlade s týmito CDPC a zabezpečí minimálne rovnakú úroveň starostlivosti s ohľadom na Dôverné informácie Poskytujúcej strany, akú Prijímajúca strana zabezpečuje na ochranu svojich vlastných Dôverných informácií podobnej povahy, ktorá však v žiadnom prípade nebude nižšia ako rozumná starostlivosť.

3. Použitie a poskytnutie Dôverných informácií

Poskytujúca strana týmto poskytuje Prijímajúcej strane právo použiť a poskytnúť Dôverné informácie Poskytujúcej strany v rozsahu nevyhnutnom na splnenie príslušných Povolených účelov. Prijímajúca strana bude mať právo použiť a poskytnúť Dôverné informácie Poskytujúcej strany len v rozsahu dovolenom v týchto CDPC.

4. Výnimky z povinnosti mlčanlivosti

Bez ohľadu na akékoľvek ustanovenie v týchto CDPC stanovujúce opak, sa obmedzenia používania a poskytovania Dôverných informácií, uvedené v týchto CDPC nevzťahujú na informácie, ktoré: (i) sú alebo sa stanú verejnými inak, ako v dôsledku neoprávneného konania alebo opomenutia Prijímajúcej strany alebo jej Spriaznených spoločností alebo ich príslušných Zástupcov pri porušení týchto CDPC; (ii) sú zákonným spôsobom získané Prijímajúcou stranou od tretej

or already known by the Receiving Party in each case without notice of any obligation to maintain it as confidential; (iii) was 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) constitutes Anonymized and/or Aggregated Data.

5. Authorised disclosures

5.1 Affiliates and Representatives. The Receiving Party may disclose the Disclosing Party's Confidential Information to the Receiving Party's Affiliates and to those of the Receiving Party's and its Affiliates' respective Representatives who have a "need to know" such Confidential Information, although only to the extent 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 5.1 shall be bound to keep such Confidential Information confidential and to use it for only the relevant Permitted Purposes.

5.2 Other disclosures. With respect to the Customer's Confidential Information, Bank Recipients may: (i) disclose it to such third parties as may be designated by the Customer (for example, the Customer's shared service centre) and to Customer Affiliates; (ii) disclose it to Payment Infrastructure Providers on a confidential basis to the extent necessary for the operation of the Account and the provision of the Services; and (iii) use it and disclose it to other Bank Recipients for the purpose of supporting the opening of accounts by, and the provision of Services to, the Customer and Customer Affiliates at and by the Bank and Bank Affiliates.

5.3 Payment reconciliation. When the Customer instructs the Bank to make a payment from an Account to a third party's account, in order to enable the third party to perform payment reconciliations, the Bank may disclose to the third party the Customer's name, address and account number (and such other Customer Confidential Information as may be reasonably required by the third party to perform payment reconciliations).

5.4 Legal and regulatory disclosure. The Receiving Party (and, where the Bank is the Receiving Party, Bank Recipients and Payment Infrastructure Providers) may disclose the Disclosing Party's Confidential Information pursuant to legal process, or pursuant to any other foreign or domestic legal and/or regulatory obligation or request, or agreement entered into by any of them and any governmental authority, domestic or foreign, or between or among any two or more domestic or foreign governmental authorities, including disclosure to courts, tribunals, and/or legal, regulatory, tax and government authorities.

6. Retention and deletion

On closure of Accounts, termination of the provision of the Services, each of the Customer and Bank Recipients shall be entitled to retain and use the other party's Confidential Information, subject to the confidentiality and security obligations herein, for legal, regulatory, audit and internal compliance purposes and in accordance with their internal records management policies to the extent that this is

strany alebo sú už známe Prijímajúcej strane bez toho, aby vedela o povinnosti zachovávať ich dôvernosť; (iii) boli nezávisle získané Prijímajúcou stranou bez toho, aby vychádzala z Dôverných informácií Poskytujúcej strany; (iv) písomne schválila oprávnená osoba Poskytujúcej strany ako informácie, ktoré môžu byť sprístupnené Prijímajúcou stranou ako nie dôverné; alebo (v) predstavujú Anonymizované a/alebo Agregované údaje.

5. Povolené spôsoby sprístupnenia

5.1 Spriaznené osoby a Zástupcovia. Prijímajúca strana môže sprístupniť Dôverné informácie Poskytujúcej strany svojim Spriazneným osobám a takým ich príslušným Zástupcom, ktorí potrebujú byť oboznámení s takými Dôvernými informáciami, avšak len v rozsahu nevyhnutnom na plnenie príslušných Povolených účelov. Prijímajúca strana zabezpečí, aby všetky Spriaznené osoby a Zástupcovia, ktorým sú sprístupnené Dôverné informácie Poskytujúcej strany v súlade s týmto článkom 5.1, boli zaviazané zachovávať dôvernosť týchto Dôverných informácií a používali ich len na príslušné Povolené účely.

5.2 Iné spôsoby sprístupnenia. S ohľadom na Dôverné informácie Klienta, Bankoví príjemcovia môžu: (i) sprístupniť ich takým tretím stranám, ktoré Klient určí (napríklad spoločnému servisnému stredisku Klienta) a Spriazneným osobám Klienta; (ii) sprístupniť ich Poskytovateľom platobnej infraštruktúry za podmienok zachovávania mlčanlivosti v rozsahu potrebnom pre vedenie Účtu a poskytovanie Služieb; a (iii) používať ich a sprístupniť ich iným Príjemcom Banky na účely podpory otvárania účtov a poskytovania služieb Klientovi a Spriazneným osobám Klienta zo strany Banky a Spriaznených osôb Banky.

5.3 Zosúladenie platieb. Keď dá Klient Banke pokyn na vykonanie platby z Účtu na účet tretej strany, môže na účely rekongiliácie platieb treťou stranou Banka poskytnúť tretej strane meno, adresu a číslo účtu Klienta (a také iné Dôverné informácie Klienta, ktoré môžu byť dôvodne požadované treťou stranou na rekongiliáciu platieb).

5.4 Sprístupnenie za účelom plnenia zákonných a regulačných povinností. Prijímajúca strana (a ak je Prijímajúcou stranou Banka, tak Príjemcovia Banky a Poskytovatelia platobnej infraštruktúry) môžu sprístupniť Dôverné informácie Poskytujúcej strany v súlade so zákonnými postupmi alebo v súlade s akýmikoľvek inými zahraničnými alebo domácimi zákonnými alebo regulačnými povinnosťami, prípadne žiadosťou, alebo zmluvou uzavretou medzi nimi a inými domácimi alebo zahraničným vládnyimi orgánmi vrátane sprístupnenia informácií súdom, tribunálom alebo regulačným, daňovým a vládnyimi orgánom.

6. Uchovávanie a likvidácia

Pri zatvorení Účtov, ukončení poskytovania Služieb budú Klient aj Príjemcovia Banky oprávnení ponechať si a použiť Dôverné informácie druhej strany pod podmienkou zachovania dôvernosti a bezpečnostných povinností podľa týchto CDPC na zákonné, regulačné účely, účely auditu alebo interného dodržiavania povinností a v súlade s ich zásadami vedenia a archivácie interných záznamov v rozsahu, ktorý je prípustný na základe

permissible under applicable laws and regulations, but shall otherwise securely destroy or delete such Confidential Information.

7. Data privacy

7.1 Compliance with law. The Receiving Party will comply with applicable Data Protection Law in Processing Disclosing Party Personal Data in connection with the provision or receipt of Accounts and Services.

7.2 Compliance with GDPR/Equivalent Laws. Without limiting Condition 7.1 (Compliance with law), to the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law: (i) each party is responsible for its own compliance with applicable Data Protection Law; and (ii) the Customer confirms that any Customer Personal Data that it provides to the Bank has been Processed fairly and lawfully, is accurate and is relevant for the purposes for which it is being provided and the Bank may rely on the Customer's compliance with such undertaking and, where applicable, assistance from the Customer pursuant to Condition 7.6 (Legal basis for Processing).

7.3 Security. The Bank will, and will use reasonable endeavors to ensure that Bank Affiliates and Third Party Service Providers will, implement reasonable and appropriate technical and organizational security measures to protect Customer Personal Data that is within its or their custody or control against unauthorized or unlawful Processing and accidental destruction or loss.

7.4 Purpose limitation. The Customer hereby authorizes the Bank to Process Customer Personal Data in accordance with these Conditions and to the extent reasonably required for the relevant Permitted Purposes for the period of time reasonably necessary for the relevant Permitted Purposes.

7.5 International transfer. The Customer acknowledges that in the course of the disclosures described in Condition 5 (Authorized disclosures), Disclosing Party Personal Data may be disclosed to recipients located in countries which do not offer a level of protection for those data as high as the level of protection in the country in which the Bank is established or the Customer is located.

7.6 Legal basis for Processing.

7.6.1 Except as noted in Condition 7.6.2:

(A) When the Customer is the Data Subject: To the extent that the Customer is the Data Subject of Customer Personal Data Processed by the Bank, then the Customer consents to the Bank's Processing of all of such Customer Personal Data as described in Conditions 3 to 7.

(B) When the Customer is not the Data Subject: To the extent that the Bank Processes Customer Personal Data about other Data Subjects (for example, the Customer's personnel or Related Parties), the Customer warrants that to the extent required by applicable law or regulation, it has provided notice to and obtained consent from such Data Subjects in relation to the Bank's Processing of their Personal Data as described in these Conditions (and will provide such notice or obtain such consent in advance of providing similar information in future). The Customer further warrants that any such consent has been granted by these Data Subjects for the period reasonably required for the realization of the relevant Permitted Purposes.

7.6.2 To the extent that the Processing of Personal Data is subject to the GDPR or any Equivalent Law then the

príslušných právnych predpisov, inak budú povinní zničiť alebo vymazať tieto Dôverné informácie.

7.Ochrana dôvernosti údajov

7.1 Dodržiavanie právnych predpisov. Prijímajúca strana bude dodržiavať všetky príslušné Predpisy o ochrane údajov pri Spracúvaní Osobných údajov Poskytujúcej strany v súvislosti s poskytovaním alebo prijatím Účtov a Služieb.

7.2 Dodržiavanie GDPR/Ekvivalentných právnych predpisov. Bez toho aby bolo dotknuté ustanovenie článku 7.1 (Dodržiavanie právnych predpisov), v rozsahu, v akom sa na Spracúvanie Osobných údajov vzťahuje GDPR alebo akékoľvek Ekvivalentné právne predpisy: (i) každá zmluvná strana bude zodpovedná za dodržiavanie príslušných Predpisov o ochrane údajov; a (ii) Klient potvrdzuje, že akékoľvek Osobné údaje Klienta, ktoré poskytne Banke boli Spracúvané správnym a zákonným spôsobom, že sú správne a týkajú sa účelov, pre ktoré sa poskytujú a že Banka sa môže spoliehať na dodržanie tohto záväzku zo strany Klienta a ak to je aplikovateľné, na asistenciu zo strany Klienta v zmysle ustanovenia článku 7.6 (Právny základ Spracúvania).

7.3 Bezpečnosť. Banka zabezpečí a vynaloží primerané úsilie na zabezpečenie toho, aby Spriaznené osoby Banky a Externí poskytovatelia služieb prijali primerané a vhodné technické a organizačné bezpečnostné opatrenia na ochranu Osobných údajov Klienta, ktoré sú v rámci jej alebo ich správy alebo pod jej alebo ich kontrolou pred neoprávneným alebo nezákonným Spracúvaním a náhodným zničením alebo stratou.

7.4 Obmedzenie účelu. Klient týmto splnomocňuje a Banku na spracovanie Osobných údajov Klienta v súlade s týmito CDPC a v rozsahu, ktorý je primerane potrebný pre príslušné Povolené účely na dobu primerane potrebnú pre príslušné Povolené účely.

7.5 Medzinárodný prenos. Klient potvrdzuje, že počas sprístupnenia údajov popísaného v článku 5 (Povolené spôsoby sprístupnenia), možno Osobné údaje Poskytujúcej strany sprístupniť príjemcom nachádzajúcim sa v krajinách, ktoré neposkytujú takú istú vysokú úroveň ochrany týchto údajov ako v krajine, v ktorej má Banka sídlo alebo v ktorej sa nachádza Klient.

7.6 Právny základ Spracúvania.

7.6.1 S výnimkou prípadov uvedených v článku 7.6.2

(A) Ak je Klient Dotknutou osobou: V rozsahu, v akom je Klient Dotknutou osobou vo vzťahu k Osobným údajom Klienta Spracúvaným zo strany Banky dáva Klient súhlas Banke so Spracúvaním všetkých takýchto Osobných údajov Klienta, ako je popísané v článkoch 3 až 7.

(B) Ak Klient nie je Dotknutou osobou: V rozsahu, v akom Banka spracúva Osobné údaje Klienta týkajúce sa iných Dotknutých osôb (napr. zamestnanci Klienta alebo Spriaznené strany), sa Klient zaväzuje, že v rozsahu, v akom to vyžadujú príslušné právne predpisy, oboznámil tieto Dotknuté osoby a získal ich súhlas so Spracúvaním ich Osobných údajov Bankou tak, ako je to uvedené v týchto CDPC (a poskytne takéto oznámenie alebo získa takýto súhlas pred poskytnutím podobných informácií aj v budúcnosti). Klient sa tiež zaručuje, že tieto Dotknuté osoby poskytli akýkoľvek takýto súhlas na obdobie primerane požadované na realizáciu príslušných Povolených účelov.

7.6.2 V rozsahu, v akom sa na Spracúvanie Osobných údajov vzťahuje GDPR alebo akékoľvek Ekvivalentné právne predpisy,

provisions of this Condition 7.6.2 shall apply:

(A) When the Customer is the Data Subject: when the Customer is the Data Subject of Customer Personal Data Processed by the Bank, then the Customer hereby acknowledges that the Bank will Process Customer Personal Data as set forth in the relevant TTS Privacy Statement accessible at www.citibank.sk (or such other URL or statement as the Bank may notify to the Customer from time to time) and the Bank may seek consent prior to conducting certain Processing activities from the Customer from time to time as its legal basis for Processing Customer Personal Data under the GDPR or any Equivalent Law; and

(B) When the Customer is not the Data Subject: when the Bank Processes Customer Personal Data about other Data Subjects (for example, the Customer's personnel or Related Parties), the Customer warrants that it shall provide notice to, and shall seek consent from (and promptly upon the Bank's request shall provide evidence to the Bank of having provided such notices and/or obtained such consents), such Data Subjects in relation to the Bank's Processing of their Personal Data in accordance with any instructions of the Bank from time to time (which may include the form and the manner in which a notice is to be provided, or any consent is to be obtained). In connection with the foregoing, the Customer warrants that it will provide Data Subjects with a copy of the relevant TTS Privacy Statement accessible at www.citibank.sk (or such other URL or statement as the Bank may notify to the Customer from time to time).

7.7 Employee reliability and training. The Bank will take reasonable steps to ensure the reliability of its employees who will have access to Customer Personal Data and will ensure that those of its employees who are involved in the Processing of Customer Personal Data have undergone appropriate training in the care, protection and handling of Personal Data.

7.8 Audit. The Bank shall provide the Customer with such information as is reasonably requested by the Customer to enable the Customer to satisfy itself of the Bank's compliance with its obligations under Condition 7.3 (Security). Nothing in this Condition 7.8 shall have the effect of requiring the Bank to provide information that may cause it to breach its confidentiality obligations to third parties.

8. Security Incidents

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 law and regulation. The Bank will notify the Customer of any Security Incident as soon as reasonably practicable after the Bank becomes aware of a Security Incident, unless the Bank is subject to a legal or regulatory constraint, or if it would compromise the Bank's investigation. The parties agree that in relation to a Security Incident, each party will be responsible for making any notifications to regulators and individuals that are required under applicable 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 Data Subjects and regulators. Neither the Bank nor the Customer will issue press or media statements or comments in connection with the Security Incident that

sa budú uplatňovať ustanovenia tohto článku 7.6.2:

(A) Ak je Klient Dotknutou osobou: ak je Klient Dotknutou osobou vo vzťahu k Osobným údajom Klienta, Spracúvaným zo strany Banky, potom Klient týmto berie na vedomie, že Banka bude Spracúvať Osobné údaje Klienta tak, ako je uvedené v príslušnom TTS Vyhlásení o ochrane osobných údajov, dostupných na www.citibank.sk (alebo na inej URL alebo v inom vyhlásení, ktoré Banka môže Klientovi z času na čas oznámiť), pričom Banka môže z času na čas požadovať súhlas Klienta pred vykonávaním určitých Spracovateľských operácií, ako právny základ pre Spracúvanie Osobných údajov Klienta podľa GDPR alebo akýchkoľvek Ekvivalentných právnych predpisov; a

(B) Ak Klient nie je Dotknutou osobou: ak Banka spracúva Osobné údaje Klienta týkajúce sa iných Dotknutých osôb (napr. zamestnanci Klienta alebo Spriaznené strany), Klient zaväzuje, že oboznámi a získa súhlas od (a bezodkladne na požiadanie Banky poskytne Banke dôkaz o poskytnutí takých oznámení a získaní takých súhlasov), takých Dotknutých osôb vo vzťahu k Spracúvaniu ich Osobných údajov Bankou v súlade s akýmkoľvek pokynom, ktorý môže Banka z času na čas vydať (a ktoré môžu zahŕňať formu a spôsob oznámenia, ktoré sa má poskytnúť alebo akéhokoľvek súhlasu, ktorý sa má získať). Vzhľadom na vyššie uvedené sa Klient zaväzuje, že poskytne Dotknutým osobám kópiu príslušného TTS Vyhlásenia o ochrane osobných údajov, dostupných na www.citibank.sk (alebo na inej URL alebo v inom vyhlásení, ktoré Banka môže Klientovi z času na čas oznámiť).

7.7 Zodpovednosť a školenie zamestnancov. Banka prijme primerané kroky na zaistenie spoľahlivosti svojich zamestnancov, ktorí majú prístup k Osobným údajom Klienta a zabezpečí, aby jej zamestnanci, ktorí sa zúčastňujú na Spracúvaní Osobných údajov Klienta, absolvovali príslušné školenie ohľadne starostlivosti, ochrany a nakladania s Osobnými údajmi.

7.8 Audit. Banka poskytne Klientovi také informácie, ako budú primerane požadované Klientom, aby mohol byť Klient oboznámený s dodržiavaním zo strany Banky jej povinností v zmysle článku 7.3 (Bezpečnosť). Žiadne ustanovenie tohto článku 7.8 nebude znamenať povinnosť pre Banku, aby poskytla informácie, ktoré by mohli spôsobiť porušenie jej záväzkov dôvernosti voči tretím osobám.

8. Bezpečnostné incidenty

Ak sa Banka dozvie o výskyte Bezpečnostného incidentu, bude zisťovať a odstráni dopady Bezpečnostného incidentu v súlade so svojou internou politikou, postupmi a požiadavkami príslušných právnych predpisov. Banka oznámi Klientovi akýkoľvek Bezpečnostný incident čo najskôr, ako to bude rozumne možné po tom, čo sa o ňom dozvie, ibaže by to podliehalo súdnym alebo regulačným obmedzeniam alebo by to mohlo ohroziť vyšetrovanie Banky. Strany súhlasia, že v súvislosti s Bezpečnostným incidentom, bude každá zmluvná strana zodpovedať za akékoľvek oznámenia regulátorom a fyzickým osobám, ktoré sú povinné v zmysle príslušných Predpisov o ochrane údajov. Každá zmluvná strana poskytne primerané informácie a súčinnosť druhej zmluvnej strane, v rozsahu nevyhnutnom na to, aby pomohla druhej zmluvnej strane splniť povinnosti voči Dotknutým osobám a regulátorom. Banka ani Klient neurobia tlačové alebo mediálne vyhlásenia alebo vyjadrenia v súvislosti s Bezpečnostným incidentom, kde by bol uvedený názov druhej strany bez predchádzajúceho

name the other party unless it has obtained the other party's prior written consent.

9. Definitions

Capitalised terms used in these Conditions shall have the meanings given to them in the Master Account and Service Terms or as set out below:

“**Affiliate**” means either a Bank Affiliate or a Customer Affiliate, as the context may require;

“**Anonymized and/or Aggregated Data**” means information relating to the Disclosing Party received or generated by the Receiving Party in connection with the provision or receipt of the Account and Services and in respect of which all direct personal identifiers have been removed, and/or which has been aggregated with other data, in both cases such that the data cannot reasonably identify the Disclosing Party, its Affiliates or a natural person;

“**Bank Affiliate**” means any entity, present or future, that directly or indirectly Controls, is Controlled by or is under common Control with the Bank, and any branch or representative offices thereof, including Citibank, N.A. and Citigroup Technologies, Inc.;

“**Bank Personal Data**” means Personal Data relating to a Data Subject received by the Customer from the Bank, Bank Affiliates and/or their respective Representatives in the course of receiving Accounts and Services from the Bank. Bank Personal Data may include names and contact details, to the extent that these amount to Personal Data under applicable Data Protection Law;

“**Bank Recipients**” means the Bank, Bank Affiliates and their respective Representatives;

“**Conditions**” means these Confidentiality and Data Privacy Conditions;

“**Confidential Information**” means:

(A) where the Disclosing Party is the Customer or a Customer Affiliate, or any of their respective Representatives: information relating to the Customer or Customer Affiliates or their respective Representatives or Related Parties received by Bank Recipients in the course of providing Accounts and Services to the Customer, including all Customer Personal Data, Customer's bank account details, transactional information, and any other information which is either designated by the Customer as confidential at the time of disclosure or that a reasonable person would consider to be of a confidential or proprietary nature; or

(B) where the Disclosing Party is the Bank or a Bank Affiliate, or any of their respective Representatives: information relating to the Bank or Bank Affiliates or their respective Representatives received or accessed by the Customer, Customer Affiliates and their respective Representatives in connection with the receipt of Accounts and Services from the Bank, including Bank Personal Data, information relating to the Bank's products and services and the terms and conditions on which they are

pisomného súhlasu druhej zmluvnej strany.

9. Definície pojmov

Pojmy používané v týchto CDPC s veľkým začiatočným písmenom budú mať rovnaký význam, ako je definovaný v Rámcových podmienkach vedenia Účtov a poskytovania Služieb, alebo ako je definovaný nižšie:

„**Spriaznená osoba**“ znamená Spriaznenú osobu Banky alebo Spriaznenú osobu Klienta v závislosti od kontextu;

„**Anonymizované alebo Agregované údaje**“ sú informácie týkajúce sa Poskytujúcej strany prijaté alebo vytvorené Prijímajúcou stranou v súvislosti s poskytovaním alebo prijímaním Účtu a Služieb, pri ktorých boli odstránené všetky priame osobné identifikačné údaje, a/alebo ktoré boli zlúčené s inými údajmi, pričom v oboch prípadoch nemožno rozumne zistiť totožnosť Poskytujúcej strany, jej Spriaznených osôb alebo fyzickej osoby;

„**Spriaznená osoby Banky**“ je akýkoľvek súčasný alebo budúci subjekt, ktorý priamo alebo nepriamo Ovláda, je Ovládaný alebo je spoločne Ovládaný Bankou alebo ich akoukoľvek pobočkou alebo zastúpením vrátane spoločností Citibank, N.A. a Citigroup Technologies, Inc.;

„**Osobné údaje Banky**“ sú Osobné údaje, týkajúce sa Dotknutej osoby prijaté Klientom od Banky, Spriaznených osôb Banky a/alebo ich príslušných Zástupcov počas prijímania Účtov a Služieb od Banky. Osobné údaje Banky môžu zahŕňať mená a kontaktné údaje v rozsahu, v akom sú považované za Osobné údaje v zmysle príslušných Predpisov o ochrane údajov;

„**Prijemcovia Banky**“ znamenajú Banku, Spriaznené osoby Banky a ich príslušných zástupcov;

„**CDPC**“ znamenajú tieto Podmienky mlčanlivosti a ochrany dôvernosti údajov;

„**Dôverné informácie**“ znamenajú:

(A) v prípade, že Poskytujúcou stranou je Klient alebo Spriaznená osoba Klienta, prípadne ich príslušní Zástupcovia: informácie týkajúce sa Klienta alebo Spriaznenej osoby Klienta alebo ich príslušných Zástupcov alebo Spriaznených strán prijaté Prijemcami Banky v priebehu poskytovania Účtov a Služieb Klientovi, vrátane všetkých Osobných údajov Klienta, údajov týkajúcich sa bankového účtu Klienta, informácií o transakciách a iných informácií, ktoré Klient označí v čase ich poskytnutia za dôverné, alebo ak ich je možné rozumne považovať príslušnou osobou za dôverné alebo súkromné; alebo

(B) v prípade, že Poskytujúcou stranou je Banka alebo Spriaznená osoba Banky, prípadne ich príslušní Zástupcovia: informácie týkajúce sa Banky alebo Spriaznenej osoby Banky alebo ich príslušných Zástupcov získané alebo sprístupnené Klientovi, spriazneným osobám Klienta a ich príslušným Zástupcom v súvislosti s prijímaním Účtov a Služieb zo strany Banky, vrátane Osobných údajov Banky, informácií týkajúcich sa produktov a služieb Banky a obchodných podmienok, na základe ktorých sú poskytované, technológie (vrátane softvéru,

provided, technology (including software, the form and format of reports and online computer screens), pricing information, internal policies, operational procedures and any other information which is either designated by the Bank as confidential at the time of disclosure or that a reasonable person would consider to be of a confidential or proprietary nature;

“**Control**” means that an entity possesses directly or indirectly the power to direct or cause the direction of the management and policies of the other entity, whether through the ownership of voting shares, by contract or otherwise;

“**Customer Affiliate**” means any entity, present or future, that directly or indirectly Controls, is Controlled by, or is under common Control with the Customer, and any branch thereof;

“**Customer Personal Data**” means Personal Data relating to a Data Subject received by or on behalf of the Bank from the Customer, Customer Affiliates and their respective Representatives and Related Parties in the course of providing Accounts and Services to the Customer. Customer Personal Data may include names, contact details, identification and verification information, nationality and residency information, taxpayer identification numbers, voiceprints, bank account and transactional information (where legally permissible), to the extent that these amount to Personal Data under applicable Data Protection Law;

“**Data Protection Law**” means any and all applicable laws and/or regulations relating to privacy and/or data protection in relation to the Processing of Customer Personal Data or Bank Personal Data, including any amendments or supplements to or replacements of such laws and/or regulations and including without limitation and as applicable: (i) the EU Directive on Data Protection (95/46/EC) and the EU Directive on Privacy and Electronic Communications (2002/58/EC); (ii) any national laws implementing such directives; (iii) the GDPR; and (iv) any Equivalent Law;

“**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 applicable Data Protection Law. For the purpose of these Conditions, Data Subjects may be the Customer, Customer Affiliates, the Bank, their personnel, Related Parties, customers, suppliers, payment remitters, payment beneficiaries or other persons;

“**Disclosing Party**” means a party that discloses Confidential Information to the other party;

“**Disclosing Party Personal Data**” means Customer Personal Data or Bank Personal Data, as the context

formy a formátu správ a počítačových obrazoviek on-line), informácií o cenách, interných predpisov, prevádzkových postupov a iných informácií, ktoré Banka označí v čase ich poskytnutia za dôverné, alebo ak ich je možné rozumne považovať príslušnou osobou za dôverné alebo súkromné;

„**Ovládanie**“ znamená, že subjekt má priamu alebo nepriamu právomoc riadiť alebo zabezpečiť riadenie a stratégiu iného subjektu, buď prostredníctvom vlastníctva akcií, s ktorými je spojené hlasovacie právo, zmluvou alebo inak;

„**Spriaznená osoba Klienta**“ akýkoľvek subjekt, súčasný alebo budúci, priamo alebo nepriamo Ovládajúci, Ovládaný alebo pod spoločným Ovládaním Klienta alebo ktoroukoľvek z jeho pobočiek;

„**Osobné údaje Klienta**“ znamenajú Osobné údaje týkajúce sa Dotknutej osoby získané zo strany Banky alebo v jej mene od Klienta, Spriaznených osôb Klienta a ich príslušných Zástupcov a Spriaznených strán v priebehu vedenia Účtov a poskytovania Služieb Klientovi. Osobné údaje Klienta môžu obsahovať mená, kontaktné údaje, identifikačné a overovacie informácie, údaje o občianstve a pobyte, daňové identifikačné čísla, záznamy hlasu, informácie o bankovom účte a transakčné informácie (tam, kde je to právne dovolené) v rozsahu, v akom sú osobnými údajmi podľa príslušných Predpisov o ochrane údajov;

„**Predpisy o ochrane údajov**“ znamenajú akékoľvek a všetky aplikovateľné zákony a/alebo predpisy týkajúce sa ochrany súkromia a/alebo osobných údajov vo vzťahu k Spracúvaniu Osobných údajov Klienta alebo Osobných údajov Banky, vrátane ich akýchkoľvek dodatkov, doplnkov alebo zákonov a/alebo predpisov, ktoré ich nahradia, vrátane najmä: (i) Smernice Európskeho parlamentu a Rady o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov (95/46/EHS) a Smernice Európskeho parlamentu a Rady o súkromí a elektronických komunikáciách (2002/58/ES); akékoľvek národné právne predpisy, ktoré implementujú tieto smernice; (iii) GDPR; a (iv) akékoľvek Ekvivalentné právne predpisy;

„**Dotknutá osoba**“ znamená fyzickú osobu, ktorá je identifikovaná alebo môže byť identifikovaná priamo alebo nepriamo, najmä odkazom na nejaký identifikátor ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor alebo na jeden alebo viac ukazovateľov špecifických pre jej fyzickú, fyziologickú, genetickú, duševnú, ekonomickú, kultúrnu alebo sociálnu identitu, alebo, ak je výraz definovaný inak, má význam výrazu pripísaný podľa príslušných Predpisov o ochrane údajov. Pre účely týchto CDPC môžu byť Dotknutými osobami Klient, Spriaznené osoby Klienta, Banka, ich zamestnanci, Spriaznené strany, zákazníci, dodávatelia, odosielatelia a prijímatelia platieb a iné osoby;

„**Poskytujúca strana**“ je strana, ktorá sprístupňuje Dôverné informácie druhej strane;

„**Osobné údaje Poskytujúcej strany**“ sú Osobné údaje Klienta alebo Osobné údaje Banky v rozsahu stanovenom daným

permits;

“Equivalent Law” means the laws and/or regulations of any country outside the EEA that are intended to provide equivalent protections for Personal Data (or the nearest equivalent term under applicable data protection law and/or regulation) of Data Subjects as the GDPR, including without limitation, the data protection laws of Jersey, Macau, Morocco, Switzerland and the United Kingdom;

“GDPR” means the General Data Protection Regulation (EU) 2016/679 and any laws and/or regulations implementing or made pursuant to such regulation;

“Payment Infrastructure Provider” means a third party which forms part of a payment system infrastructure, including without limitation communications, clearing or payment systems, intermediary banks and correspondent banks;

“Permitted Purposes” in relation to the Bank’s use of the Customer’s Confidential Information means the following purposes: (A) to provide Accounts and Services to the Customer in accordance with the Terms; (B) to undertake activities related to the provision of Accounts and Services, such as, by way of non-exhaustive example: (1) to fulfil foreign and domestic legal, regulatory and compliance requirements (including US anti-money laundering obligations applicable to the Bank’s parent companies) and comply with any applicable treaty or agreement with or between foreign and domestic governments applicable to any of the Bank, Bank Affiliates and their agents or Payment Infrastructure Providers; (2) to verify the identity of Customer representatives who contact the Bank or may be contacted by the Bank; (3) for risk assessment, information security management, statistical, trend analysis and planning purposes; (4) to monitor and record calls and electronic communications with the Customer for quality, training, investigation and fraud prevention purposes; (5) for crime detection, prevention, investigation and prosecution; (6) to enforce or defend the Bank’s or Bank Affiliates’ rights; and (7) to manage the Bank’s relationship with the Customer, which may include providing information to Customer and Customer Affiliates about the Bank’s and Bank Affiliates’ products and services; (C) the purposes set out in Condition 5 (Authorised disclosures); (D) any additional purposes expressly authorised by the Customer; and (E) any additional purposes as may be notified to the Customer or Data Subjects in any notice provided by, or upon the instruction of, the Bank pursuant to Condition 7.6.2;

“Permitted Purposes” in relation to the Customer’s use of the Bank’s Confidential Information means the following purposes: to enjoy the benefit of, enforce or defend its rights and perform its obligations in connection with the receipt of Accounts and Services from the Bank in accordance with the Terms, and to manage the Customer’s relationship with the Bank;

kontextom;

„Ekvivalentné právne predpisy“ znamenajú zákony a/alebo predpisy ktorejkoľvek krajiny nachádzajúcej sa mimo EHP, ktoré majú za cieľ poskytnúť ekvivalentnú ochranu Osobných údajov (alebo najbližšiemu ekvivalentnému pojmu podľa príslušných zákonov a/alebo predpisov o ochrane osobných údajov) Dotknutých osôb ako GDPR, vrátane najmä právnych predpisov o ochrane osobných údajov v Jersey, Macau, Maroku, Švajčiarsku a v Spojenom kráľovstve;

„GDPR“ znamená Nariadenie Európskeho parlamentu a Rady (EU) o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) a akýkoľvek právny predpis implementujúci toto nariadenie alebo vydaný na jeho základe;

„Poskytovateľ platobnej infraštruktúry“ znamená tretiu osobu, ktorá je súčasťou systému platobnej infraštruktúry vrátane, ale nie výlučne, komunikačných, zúčtovacích alebo platobných systémov, sprostredkovateľských a korešpondenčných bánk;

„Povolené účely“ v súvislosti s používaním Dôverných informácií Klienta Bankou znamenajú tieto účely: (A) vedenie Účtov a poskytovanie Služieb Klientovi v súlade s Podmienkami; (B) vykonávanie činností súvisiacich s vedením Účtov a poskytovaním Služieb, ako napríklad: (1) plnenie zahraničných a domácich zákonných, regulačných požiadaviek a compliance povinností (vrátane povinností podľa predpisov USA týkajúcich sa boja proti legalizácii príjmu z trestnej činnosti vzťahujúcich sa na materské spoločnosti Banky) a dodržiavanie akejkoľvek príslušnej dohody alebo zmluvy medzi zahraničnými a domácimi vládami, ktoré sa vzťahujú na Banku, Spriaznené osoby Banky a ich zástupcov alebo Poskytovateľov platobnej infraštruktúry; (2) overenie totožnosti zástupcov Klienta, ktorí kontaktujú Banku alebo môžu byť kontaktovaní Bankou; (3) Pre účely posúdenia rizika, riadenie bezpečnosti informácií, štatistické analýzy, analýzy trendov a účely plánovania; (4) na sledovanie a zaznamenávanie telefonátov a elektronickej komunikácie s Klientom na účely zabezpečovania kvality, školenia, vyšetrovania a prevencie pred podvodmi; (5) na odhaľovanie, prevenciu, vyšetrovanie a stíhanie trestných činov; (6) na vymáhanie a obhajovanie práv Banky alebo Spriaznených osôb Banky a (7) na riadenie vzťahov Banky s Klientom, ku ktorému môže patriť poskytovanie informácií Klientovi a Spriazneným osobám Klienta o produktoch a službách Banky alebo Spriaznených osôb Banky; (C) účely uvedené v článku 5 (Povolené spôsoby prístupnosti); (D) akékoľvek ďalšie účely, výslovne odsúhlasené zo strany Klienta; a (E) akékoľvek ďalšie účely, ktoré môžu byť oznámené Klientovi alebo Dotknutým osobám v akomkoľvek oznámení poskytnutom zo strany Banky alebo na základe jej inštrukcie v zmysle článku 7.6.2;

„Povolené účely“ v súvislosti s používaním Dôverných informácií Banky Klientom znamenajú nasledujúce účely: využívanie výhod, vymáhanie alebo obranu jeho práv a plnenie jeho povinností v súvislosti s vedením Účtov a poskytovaním Služieb od Banky v súlade s Podmienkami a na riadenie vzťahu Klienta s Bankou;

“**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 applicable 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, 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 applicable Data Protection Law;

“**Receiving Party**” means a party that receives Confidential Information from the other party;

“**Related Party**” means any natural person or entity, or branch thereof, that: (i) owns, directly or indirectly, stock of the Customer, if the Customer is a corporation, (ii) owns, directly or indirectly, profits, interests or capital interests in the Customer, if the Customer is a partnership, (iii) is treated as the owner of the Customer, if the Customer is a “grantor trust” under sections 671 through 679 of the United States Internal Revenue Code or is of equivalent status under any similar law of any jurisdiction, domestic or foreign, (iv) holds, directly or indirectly, beneficial interests in the Customer, if the Customer is a trust; or (v) exercises control over the Customer directly or indirectly through ownership or any arrangement or other means, if the Customer is an entity, including: (a) a settlor, protector or beneficiary of a trust; (b) a person who ultimately has a controlling interest in the Customer; (c) a person who exercises control over the Customer through other means; or (d) the senior managing official of the Customer;

“**Representatives**” means a party’s officers, directors, employees, agents, representatives, professional advisers and Third Party Service Providers;

“**Security Incident**” means an incident whereby the confidentiality of Disclosing Party Personal Data within Receiving Party’s custody or control has been materially compromised so as to pose a reasonable likelihood of harm to the Data Subjects involved; and

“**Third Party Service Provider**” means a third party reasonably 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 Infrastructure Provider. Examples of Third Party Service Providers include technology service providers, business process outsourcing service providers and call center service providers.

Treasury and Trade Solutions

Confidentiality and Data Privacy Conditions (Global)_v.1.6 (March 2018)
© 2018 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.
citi.com/treasuryandtradesolutions

„**Osobné údaje**“ znamenajú akúkoľvek informáciu, ktorá môže byť použitá, priamo alebo nepriamo, samostatne alebo v kombinácii s inou informáciou na identifikáciu Dotknutej osoby, alebo, ak je výraz definovaný inak, má význam výrazu pripísaný podľa príslušných Predpisov o ochrane údajov;

„**Spracúvanie**“ znamená vykonávanie akýchkoľvek operácií alebo súboru operácií s Osobnými údajmi alebo súbormi Osobných údajov, automatizovanými prostriedkami alebo bez nich, napr. ich zhromažďovanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, konzultovanie, využívanie, sprístupnenie prenosom, rozširovanie alebo iné sprístupňovanie, zoradenie alebo kombinovanie, obmedzovanie, výmaz alebo likvidáciu, alebo, ak je výraz definovaný inak, má význam výrazu pripísaný podľa príslušných Predpisov o ochrane údajov;

„**Prijímajúca strana**“ je strana, ktorá prijíma Dôverné informácie od druhej strany;

„**Spriaznená strana**“ je akákoľvek fyzická osoba alebo subjekt alebo ich pobočka, ktorá: (i) priamo alebo nepriamo vlastní akcie Klienta, ak je Klient spoločnosťou, (ii) priamo alebo nepriamo vlastní zisky, podiely alebo kapitálové podiely Klienta, ak je Klient združením, (iii) sa považuje za vlastníka Klienta, ak je Klient „zakladateľ trustu“ na základe § 671 až 679 Kódexu Spojených štátov amerických o domácich príjmoch alebo má ekvivalentný štatút na základe obdobných právnych predpisov akejkoľvek domácej alebo zahraničnej jurisdikcie, (iv) priamo alebo nepriamo vlastní konečné výhody týkajúce sa Klienta, ak je Klient trustom; alebo (v) priamo alebo nepriamo ovláda Klienta prostredníctvom vlastníctva, inej dohody alebo iných prostriedkov, ak je Klient subjektom vrátane: (a) zriaďovateľa, správcu alebo beneficianta trustu; (b) osoby, ktorá má na najvyššej úrovni rozhodujúci podiel v Klientovi; (c) osoby, ktorá ovláda Klienta prostredníctvom iných prostriedkov; alebo (d) člena vyššieho manažmentu Klienta;

„**Zástupcovia**“ znamenajú úradníkov, riaditeľov, zamestnancov, konateľov, zástupcov, odborných poradcov strany a Externých poskytovateľov služieb;

„**Bezpečnostný incident**“ znamená incident, kedy došlo k podstatnému ohrozeniu dôvernosti Osobných údajov Poskytujúcej strany v správe alebo pod kontrolou Prijímajúcej strany, ktorý predstavuje odôvodnenú pravdepodobnosť poškodenia Dotknutých osôb, ktorých sa to týka; a

„**Externý poskytovateľ služieb**“ znamená tretiu osobu primerane vybranú Prijímajúcou stranou alebo jej Spriaznenou osobou za účelom poskytovania služieb alebo v prospech Prijímajúcej strany a ktorá nie je Poskytovateľom platobnej infraštruktúry. Príklady Externých poskytovateľov služieb zahŕňajú poskytovateľov technologických služieb, poskytovateľov služieb outsourcingu business procesov a poskytovateľov služieb call centra.

Treasury and Trade Solutions

Podmienky mlčanlivosti a ochrany dôvernosti údajov (Global)_v.1.6 (Marec 2018)
© 2018 Citibank, N.A. Všetky práva vyhradené.
Citi a Citi s dizajnom Oblúka sú ochranné známky alebo servisné známky Citigroup Inc. alebo jej spriaznených osôb a sú celosvetovo používané a registrované.
citi.com/treasuryandtradesolutions