

Confidentiality and Data Privacy Conditions

Podmienky mlčanlivosti a ochrany dôvernosti údajov

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.

1. Úvod

Tieto podmienky („**Podmienky**“) vysvetľujú, ako môže každá strana používať a ako musí chrániť Dôverné informácie druhej strany (vrátane Osobných údajov) v súvislosti s poskytovaním účtov a iných produktov a služieb, či už súvisiacich s účtami, alebo nie, zo strany Banky a s ich používaním zo strany Klienta (ďalej spoločne ako „**Služby**“). „**Banka**“ má význam uvedený v zmluvných podmienkach, ktoré tieto Podmienky do seba zhŕňajú alebo na nich inak odkazujú.

2. Ochrana Dôverných Informácií

2.1 Definície pojmov

„**Dôverné informácie**“ znamenajú informácie (v hmotnej alebo nehmotnej podobe) týkajúce sa poskytovajúcej strany a / alebo jej spriaznených osôb (vrátane akéhokoľvek subjektu, ktorý priamo alebo nepriamo ovláda, je ovládaný alebo je spoločne ovládaný takou stranou) pobočiek alebo zástupcov (ďalej spoločne ako „**Spriaznené osoby**“) alebo ich príslušných Zástupcov alebo Vlastníkov, ktoré prijímajúca strana alebo jej Spriaznené osoby alebo ich príslušní Zástupcovia prijímajú alebo k nim majú prístup v súvislosti s poskytovaním, prijímaním alebo využívaním Služieb. „Dôverné informácie“ zahŕňajú Osobné údaje, informácie týkajúce sa produktov a služieb Banky a podmienky, za ktorých sú poskytované, technológie (vrátane softvéru, formy a formátu správ a počítačových obrazoviek on-line), informácie o cenách, interné predpisy, prevádzkové postupy, podrobnosti o bankových účtoch, informácie o transakciách a akéhokoľvek ďalšie informácie, ktoré v každom prípade: (i) poskytovajúca strana označí v čase ich poskytnutia za dôverné; (ii) sú chránené ako bankové tajomstvo alebo inými príslušnými právnymi predpismi; alebo (iii) rozumná osoba by ich považovala za dôverné a / alebo súkromné, vzhľadom na povahu informácií a okolnosti ich sprístupnenia.

“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 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.

„Vlastník“ je každá fyzická osoba alebo subjekt (alebo jeho pobočka), ktorá: (i) priamo alebo nepriamo vlastní akcie alebo výnosy, podiely alebo kapitál alebo iné výhody v zmluvnej strane; alebo (ii) inak vlastní alebo vykonáva kontrolu nad touto stranou priamo alebo nepriamo prostredníctvom vlastníctva, kontrolného podielu alebo akýmkoľvek iným dojednaním alebo spôsobom vrátane: (a) osoby, ktorá má v konečnom dôsledku kontrolný podiel alebo inak vykonáva kontrolu nad touto stranou; alebo b) vedúcich riadiacich zamestnancov tejto strany.

„Zástupcovia“ znamenajú vedúcich zamestnancov, riaditeľov, zamestnancov, zmluvných partnerov, konateľov, zástupcov, odborných poradcov a Externých poskytovateľov služieb tej ktorej strany;

2.2 Ochrana

Prijímajúca strana bude uchovávať Dôverné informácie poskytujúcej strany ako dôverné v súlade s týmito Podmienkami a zabezpečí minimálne rovnakú úroveň starostlivosti s ohľadom na Dôverné informácie poskytujúcej strany, akú prijímajúca strana zabezpečuje na ochranu svojich vlastných Dôverných informácií obdobnej povahy, ktorá však v žiadnom prípade nebude v nižšom rozsahu ako je rozumná starostlivosť. Prijímajúca strana bude mať právo použiť a poskytnúť Dôverné informácie poskytujúcej strany len v rozsahu povolenom v týchto Podmienkach.

2.3 Výnimky z povinnosti dodržiavať mlčanlivosť

Bez ohľadu na akékoľvek ustanovenie v týchto Podmienkach stanovujúce opak, avšak za podmienok stanovených Predpismi o ochrane údajov, sa obmedzenia používania a poskytovania Dôverných informácií, uvedené v týchto Podmienkach nevzťahujú na informácie, ktoré: (i) sú alebo sa stanú verejnými inak, ako v dôsledku neoprávneného konania alebo opomenutia prijímajúcej strany alebo jej Spriaznených osôb alebo ich príslušných Zástupcov pri porušení týchto Podmienok; (ii) sú zákonným spôsobom získané prijímajúcou stranou od tretej 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) boli anonymizované a / alebo agregované s inými informáciami tak, aby neboli odhalené Dôverné informácie poskytujúcej strany ani totožnosť žiadnej Dotknutej osoby.

3. Authorized Disclosure

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 fulfil 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);

3. Povolené spôsoby sprístupnenia

3.1 Definície pojmov

„**Príjemcovia Banky**“ znamenajú Banku, Spriaznené osoby Banky a ich príslušných Zástupcov.

„**Sprostredkovateľ platieb**“ znamená tretiu osobu, ktorá je súčasťou systému infraštruktúry platobných systémov alebo ktorá inak sprostredkuje vykonávanie platieb, vrátane najmä: komunikačných, zúčtovacích a iných platobných systémov alebo obdobných poskytovateľov služieb; sprostredkovateľských a korešpondenčných bánk, agentov; poskytovateľov digitálnych alebo elektronických peňaženiek; alebo obdobných subjektov.

„**Povolené účely**“ znamenajú v súvislosti s používaním Dôverných informácií jednej strany (alebo jej Spriaznených osôb alebo ich príslušných Zástupcov) druhou stranou (alebo jej Spriaznenými osobami alebo ich príslušnými Zástupcami):

(A) Poskytovanie, alebo prijímanie a používanie Služieb v súlade s príslušnými zmluvnými podmienkami a vykonávanie súvisiacich činností, ako sú príkladom uvedené nižšie:

(1) Plnenie príslušných domácich a zahraničných zákonných, regulačných a compliance požiadaviek (vrátane povinností týkajúcich sa pravidiel Poznaj svojho klienta (Know Your Customer) a požiadaviek týkajúcich sa boja proti legalizácii príjmu z trestnej činnosti (AML) vzťahujúcich sa na danú stranu a/alebo jej Spriaznené osoby) a iné sprístupnenia uvedené v článku 3.3 (Sprístupnenie za účelom plnenia zákonných a regulačných povinností);

(2) Overenie totožnosti Zástupcov strany, ktorí konajú s druhou stranou, vrátane ich oprávnenia konať;

(3) Pre účely posúdenia rizika, riadenie bezpečnosti informácií, štatistické analýzy, analýzy trendov a účely plánovania;

(4) Sledovanie a zaznamenávanie telefonátov a elektronickej komunikácie s druhou stranou na účely zabezpečovania kvality, školenia, vyšetrovania a prevencie pred podvodmi a inými trestnými činmi;

(5) Odhaľovanie, prevenciu, vyšetrovanie a stíhanie podvodov a iných trestných činov;

(6) Vymáhanie a obhajovanie práv príslušnej strany alebo jej Spriaznených osôb; a

(7) Riadenie vzťahov príslušnej strany s druhou stranou (čo môže zahŕňať poskytovanie informácií Klientovi a Spriazneným osobám Klienta zo strany Banky o produktoch a službách Banky alebo Spriaznených osôb Banky);

- (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 fulfill 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

- (B) Sprístupňovať informácie tretím stranám, v súvislosti s účtami ktorých Klient zadá Banke alebo Spriazneným osobám Banky pokyn vykonať alebo prijať platbu z účtu alebo umožniť takýmto tretím stranám vykonať vyrovnanie platieb;
- (C) Sprístupňovať informácie Sprostredkovateľom platieb a Externým poskytovateľom služieb na strane Banky alebo Spriaznených osôb Banky v súvislosti s poskytovaním Služieb;
- (D) Sprístupňovať informácie a získavať informácie od úverových informačných registrov, ratingových agentúr, centrálnych bánk alebo iných orgánov v súvislosti s analýzou a rozhodnutiami Banky založenými na posudzovaní rizík, alebo ak sa takéto sprístupnenie inak vyžaduje podľa príslušných právnych predpisov;
- (E) Sprístupňovať informácie Spriazneným osobám sprístupňujúcej strany a povereným tretím osobám;
- (F) V súvislosti s poskytovaním produktov a služieb (vrátane podpory otvárania účtov) Bankou a Spriaznenými osobami Banky pre Spriaznené osoby Klienta; a
- (G) Pre akékoľvek iné ďalšie účely, výslovne povolené druhou stranou.
- „**Externý poskytovateľ služieb**“ znamená tretiu osobu vybranú prijímajúcou stranou alebo jej Spriaznenou osobou za účelom poskytovania služieb pre alebo v prospech prijímajúcej strany a ktorá nie je Sprostredkovateľom platieb (napríklad poskytovateľa technologických služieb, poskytovateľa služieb business procesov, poskytovateľa služieb call centra, poskytovateľa služieb outsourcingu, konzultanti a iní externí poradcovia).

3.2 Povolené sprístupnenie

Poskytujúca strana súhlasí (a ak to vyžadujú príslušné právne predpisy týkajúce sa ochrany bankového tajomstva alebo iné príslušné právne predpisy, tak sa to bude považovať za vzdanie sa práva alebo súhlas tejto strany tak, aby sa zabezpečilo), že prijímajúca strana môže použiť a sprístupniť Dôverné informácie poskytujúcej strany Spriazneným osobám prijímajúcej strany a jej a ich príslušným Zástupcom, Sprostredkovateľom platieb a akýmkoľvek iným príjemcov tretích strán uvedených v týchto Podmienkach, ktorí požadujú prístup k takýmto Dôverným informáciám v rozsahu, ktorý je rozumne potrebný na splnenie príslušných Povolených účelov. Prijímajúca strana zabezpečí, aby všetky Spriaznené

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.

osoby a Zástupcovia, ktorým sú sprístupnené Dôverné informácie poskytovajúcej strany v súlade s týmto článkom 3.2, boli zaviazaní zachovávať dôvernosc týchto Dôverných informácií a používali ich len na príslušné Povolené účely.

3.3 Sprístupnenie za účelom plnenia zákonných a regulačných povinností

Poskytovajúca strana súhlasí (a ak to vyžadujú príslušné právne predpisy týkajúce sa ochrany bankového tajomstva alebo iné príslušné právne predpisy, tak sa to bude považovať za vzdanie sa práva alebo súhlas tejto strany tak, aby sa zabezpečilo), že prijímajúca strana (a v prípade, ak je prijímajúcou stranou Banka tak Prijemcovia Banky a Sprostredkovatelia platieb) môže použiť a sprístupniť Dôverné informácie poskytovajúcej strany na základe: (i) zákonných postupov, (ii) akéhokoľvek domáceho alebo zahraničného právneho alebo regulačného povolenia, povinnosti alebo požiadavky, (iii) zmluvy uzavretej medzi nimi a akýmikoľvek domácimi alebo zahraničnými vládnyimi orgánmi, alebo (iv) medzi akýmikoľvek dvoma alebo viacerými domácimi alebo zahraničnými vládnyimi orgánmi, vrátane sprístupnenia informácií súdom, tribunálom alebo regulačným, daňovým a vládnyimi orgánom.

4. Doba uchovávania

Každý z Prijemcov Klienta a Banky môže uchovávať, používať a podľa potreby Spracúvať Dôverné informácie druhej strany na dobu primerane potrebnú pre naplnenie príslušných Povolených účelov. Pri ukončení poskytovania Služieb (vrátane zatvorenia účtov) budú Prijemcovia Klienta aj Prijemcovia Banky oprávnení ponechať si, použiť a podľa potreby Spracúvať Dôverné informácie druhej strany na zákonné, regulačné účely, účely auditu alebo dodržiavania povinností týkajúcich sa compliance a v súlade s ich zásadami vedenia a archivácie interných záznamov v rozsahu, ktorý je prípustný na základe príslušných právnych predpisov, a inak v súlade s ustanoveniami týchto Podmienok, inak budú povinní bezpečne zničiť alebo vymazať tieto Dôverné informácie.

5. Informačná bezpečnosť

Banka zabezpečí, a vynaloží primerané úsilie na zabezpečenie toho, aby aj Spriaznené osoby Banky a Externí poskytovatelia služieb rovnako zabezpečili prijatie primeraných a vhodných fyzických, technických a organizačných bezpečnostných opatrení na ochranu Dôverných informácií Klienta, ktoré sú v rámci jej alebo ich správy alebo pod jej alebo ich kontrolou pred neoprávneným alebo nezákonným použitím (alebo v prípade Osobných údajov neoprávneným Spracúvaním) a náhodným zničením alebo stratou.

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. Osobné údaje

6.1 Definície pojmov

„**Predpisy o ochrane údajov**“ znamenajú akékoľvek a všetky aplikovateľné zákony a/alebo predpisy, týkajúce sa ochrany súkromia a osobných údajov vo vzťahu k Spracúvaniu Osobných údajov, vrátane ich akýchkoľvek dodatkov, doplnkov alebo predpisov, ktoré ich nahradia.

„**Dotknutá osoba**“ znamená fyzickú osobu, ktorá je identifikovaná alebo môže byť identifikovateľná 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 tento výraz definovaný inak, má význam ako taký výraz, ktorý je definovaný podľa Predpisov o ochrane údajov, alebo ako iný, jemu významom najbližší definovaný výraz.

„**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 tento výraz definovaný inak, má význam ako taký výraz, ktorý je definovaný podľa Predpisov o ochrane údajov, alebo ako iný, jemu významom najbližší definovaný výraz.

„**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, štrukturovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, konzultovanie, využívanie, sprístupnenie prenosom, rozširovanie alebo iné sprístupňovanie, zoradenie alebo kombinovanie, obmedzovanie, výmaz alebo likvidáciu, alebo, ak je tento výraz definovaný inak, má význam ako taký výraz, ktorý je definovaný podľa Predpisov o ochrane údajov, alebo ako iný, jemu významom najbližší definovaný výraz.

„**Bezpečnostný incident**“ znamená udalosť, kedy v dôsledku porušenia týchto Podmienok došlo k podstatnému ohrozeniu dôvernosti Osobných údajov poskytujúcej strany v správe alebo pod kontrolou prijímajúcej strany, a ktorá predstavuje odôvodnenú pravdepodobnosť poškodenia Dotknutých osôb, ktorých sa týka.

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.

6.2 Dodržiavanie Predpisov o ochrane údajov

V súvislosti s poskytovaním alebo prijímaním a využívaním Služieb: (i) každá strana bude dodržiavať Predpisy o ochrane údajov; a (ii) Klient potvrdzuje, že všetky Osobné údaje, ktoré poskytuje Príjemcom Banky, boli Spracúvané správnym a zákonným spôsobom, sú presné a sú relevantné pre účely, na ktoré sa poskytujú.

6.3 Cezhraničné prenosy Osobných údajov

Klient berie na vedomie a, ak to vyžadujú príslušné právne predpisy, súhlasí s tým, že v súvislosti s poskytovaním Služieb a iným sprístupňovaním informácií v súlade s článkom 3 (Povolené spôsoby sprístupnenia), Osobné údaje Dotknutých osôb Klienta (napríklad Zástupcov a Vlastníkov Klienta alebo jeho Spriaznených osôb), môžu byť sprístupnené a / alebo prenesené príjemcom nachádzajúcim sa v iných krajinách, ako je krajina, v ktorej je umiestnená alebo založená Banka alebo jej pobočka, ktorá poskytuje Služby alebo v ktorej sa nachádza Klient. Banka však: (i) vyžaduje, aby aj jej Spriaznené osoby a Externí poskytovatelia služieb chránili Osobné údaje v súlade s ustanoveniami článku 5 (Informačná bezpečnosť); a (ii) vykonáva cezhraničné prenosy Osobných údajov v súlade s Predpismi o ochrane údajov.

6.4 Právny základ Spracúvania Osobných údajov

V rozsahu, v akom Banka Spracúva Osobné údaje Dotknutých osôb Klienta, sa Klient zaväzuje, že v rozsahu, v akom to vyžadujú Predpisy o ochrane údajov (ak to vyžadujú), oboznámi tieto Dotknuté osoby a získal ich súhlas so Spracúvaním ich Osobných údajov Bankou tak, ako je to uvedené v týchto Podmienkach a v akomkoľvek príslušnom Vyhlásení o ochrane osobných údajov Banky alebo iných zverejnených vyhláseniach, týkajúcich sa ochrany súkromia, ktoré sú prístupné na webovej adrese <https://www.citibank.com/tts/sa/tts-privacy-statements/index.html> (alebo na inej URL adrese alebo v inom vyhlásení, ktoré môže Banka z času na čas Klientovi oznámiť). Ak je Dotknutou osobou samotný Klient, Klient týmto vyhlasuje, že v rozsahu, v akom to vyžadujú Predpisy o ochrane údajov (ak to vyžadujú): (a) obdržal informácie týkajúce sa ochrany súkromia, uvedené v predchádzajúcej vete; a (b) súhlasí s takým Spracúvaním.

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.

6.5 Bezpečnostné incidenty

(A) Ak sa Banka dozvie o výskyte Bezpečnostného incidentu, bude zisťovať a odstráni dopady Bezpečnostného incidentu v súlade so svojimi vnútornými predpismi, 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 také oznámenie podliehalo súdnym alebo regulačným obmedzeniam alebo ak by to mohlo ohroziť prebiehajúce vyšetrovanie Banky.

(B) Každá strana bude zodpovedať za akékoľvek oznámenia regulátorom a Dotknutým osobám v súvislosti s Bezpečnostným incidentom, ktoré je potrebné vykonať v zmysle Predpisov o ochrane údajov. Každá strana poskytne primerané informácie a súčinnosť druhej strane v rozsahu nevyhnutnom na to, aby pomohla druhej strane splniť jej záväzky voči regulátorom a Dotknutým osobám.

(C) Žiadna strana nevykoná žiadne tlačové alebo mediálne vyhlásenia alebo vyjadrenia v súvislosti s Bezpečnostným incidentom, ktoré budú označovať menom druhú stranu bez predchádzajúceho písomného súhlasu druhej strany.