Confidentiality and Data Privacy Conditions
Порядок обеспечения конфиденциальности информации и защиты данных

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.

1. Введение.

В настоящем Порядке обеспечения конфиденциальности информации и защиты данных (далее – «**Порядок обеспечения конфиденциальности**») разъясняется, каким образом каждая из сторон может использовать и должна защищать Конфиденциальную информацию другой стороны (включая Персональные данные) в связи с предоставлением Банком и получением и использованием Клиентом банковских счетов, а также связанных или не связанных с банковскими счетами продуктов и услуг (далее – «**Услуги**»). Термин «**Банк**» имеет значение, установленное в тех или иных правилах и условиях, включающих в себя настоящий Порядок обеспечения конфиденциальности либо содержащих отсылку к нему.

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.

2. Защита Конфиденциальной информации.

2.1 Термины и определения.

«**Конфиденциальная информация**» – информация на материальных или нематериальных носителях, касающаяся раскрывающей стороны и/или ее аффилированных лиц (включая любое лицо, которое прямо или опосредованно контролирует другое лицо, контролируется другим лицом или вместе с другим лицом находится под общим контролем иного лица), филиалов, представительств (вместе – «**Аффилированные лица**») или их соответствующих Представителей или Владельцев, которая получена принимающей стороной, ее Аффилированными лицами или их соответствующими Представителями либо становится иным образом доступной им в связи с предоставлением, получением или использованием Услуг. Конфиденциальная информация включает в себя Персональные данные, информацию, касающуюся продуктов и услуг Банка и правил и условий их предоставления, технологий (включая программное обеспечение, формы и форматы отчетов и онлайн-экранов компьютеров), информацию о ценах, внутренние политики, операционные процедуры, реквизиты банковских счетов, транзакционную информацию, а также любую другую информацию, которая в каждом конкретном случае: (i) определена раскрывающей стороной как конфиденциальная на момент раскрытия; (ii) защищена законодательством о банковской тайне или иными нормативными правовыми актами; или (iii) которую разумное лицо рассматривало бы как конфиденциальную и/или составляющую

коммерческую тайну, учитывая характер информации и обстоятельства ее раскрытия.

"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.

«**Владелец**» – любое физическое или юридическое лицо (или филиал юридического лица), которое: (i) прямо или опосредованно владеет акциями, прибылью или капиталом какого-либо лица или бенефициарным интересом в нем; или (ii) иным образом владеет каким-либо лицом или контролирует его прямо или опосредованно через право собственности, контрольный пакет акций или любым другим способом, включая: (a) лицо, которое в конечном итоге имеет контрольный пакет акций какого-либо лица или иным образом контролирует это лицо; или (b) старшее(-ие) должностное(-ые) лицо(-а) какого-либо лица.

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

«Представители» – должностные лица, директора, сотрудники, подрядчики, агенты, представители, профессиональные консультанты и Сторонние поставщики услуг какой-либо стороны.

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.

2.2 Защита Конфиденциальной информации. Принимающая сторона обязана обеспечить защиту Конфиденциальной информации раскрывающей стороны в соответствии с настоящим Порядком обеспечения конфиденциальности и проявлять по меньшей мере ту же степень заботливости и осмотрительности в отношении Конфиденциальной информации раскрывающей стороны, какую принимающая сторона проявляет для защиты своей собственной Конфиденциальной информации аналогичного характера, но в любом случае действуя как минимум с надлежащей степенью заботливости и осмотрительности. Принимающая сторона может использовать и раскрывать Конфиденциальную информацию раскрывающей стороны только в той степени, в которой это допускается настоящим Порядком обеспечения конфиденциальности.

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

2.3 Исключения из режима конфиденциальности. Невзирая на какие-либо положения настоящего Порядка обеспечения конфиденциальности об обратном, но с учетом требований Законодательства о защите данных, предусмотренные в настоящем Порядке обеспечения конфиденциальности ограничения на использование и раскрытие Конфиденциальной информации не распространяются на информацию, которая: (i) является или становится общедоступной, кроме как вследствие неправомерного действия или бездействия принимающей стороны, ее Аффилированных лиц или их соответствующих Представителей, действующих в нарушение настоящего Порядка обеспечения конфиденциальности; (ii) законным образом получена принимающей стороной от третьего

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.

лица либо уже известна принимающей стороне, причем в каждом из этих случаев без каких-либо обязательств по соблюдению конфиденциальности принимающей стороной; (iii) самостоятельно разработана принимающей стороной без ссылки на Конфиденциальную информацию раскрывающей стороны; (iv) письменно согласована уполномоченным должностным лицом раскрывающей стороны как информация, которая может раскрываться принимающей стороной на неконфиденциальной основе; или (v) была анонимизирована и/или агрегирована с другой информацией таким образом, что ни Конфиденциальная информация раскрывающей стороны, ни личность какого-либо Субъекта данных не разглашаются.

3. Authorized Disclosures.

3. Разрешенное раскрытие информации.

3.1 Definitions.

3.1 Термины и определения.

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

«**Банковские получатели**» – Банк, Аффилированные лица Citigroup Inc и их соответствующие Представители.

"Payment Facilitator" means a third party which 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; and intermediary, agent and correspondent banks; digital or ewallets; or similar entities.

«**Платежный посредник**» – третье лицо, которое является частью инфраструктуры платежной системы или иным образом обслуживает платежи, в том числе, среди прочего, телекоммуникационные, клиринговые и другие расчетные системы или поставщики аналогичных услуг, банки-посредники, банки-агенты, банки-корреспонденты, цифровые или электронные кошельки и аналогичные организации.

"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:

«**Разрешенные цели**» означает в отношении использования одной стороной (или ее Аффилированными лицами, или их соответствующими Представителями) Конфиденциальной информации другой стороны (или ее Аффилированных лиц, или их соответствующих Представителей) следующее:

(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:

(A) Предоставление или получение и использование Услуг в соответствии с регулирующими их правилами и условиями и осуществление связанных с этим действий, включающих в себя, среди прочего:

(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);

(1) Выполнение применимых требований национального и иностранного законодательства, комплаенс-контроля (в том числе применимых к соответствующей стороне и/или ее Аффилированным лицам процедур «знай своего клиента» и политики противодействия отмыванию денежных средств), а также раскрытие информации в соответствии с п. 3.3 *(Раскрытие информации по требованию уполномоченных органов)* настоящего Порядка обеспечения конфиденциальности;

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

(2) Подтверждение личности или полномочий Представителей одной стороны, осуществляющих взаимодействие с другой стороной;

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

(3) Оценка рисков, управление информационной безопасностью, статистический анализ, тренд-анализ, планирование;

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

(4) Контроль и запись телефонных переговоров и электронных сообщений между сторонами в целях обеспечения качества, обучения персонала, проведения расследования, предупреждения мошенничества и иных преступлений;

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

(5) Предупреждение, выявление, расследование мошеннических операций и иных преступлений и уголовное преследование виновных лиц;

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

(6) Обеспечение и защита прав стороны или ее Аффилированных лиц; и

(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);

(7) Управление отношениями одной стороны с другой стороной (что может включать в себя предоставление Банком Клиенту и его Аффилированным лицам информации о продуктах и услугах Банка и его Аффилированных лиц).

(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;

(B) Раскрытие информации третьим лицам, на счета которых Клиент поручает Банку или его Аффилированным лицам произвести или получить платеж со счета, либо предоставление таким третьим лицам возможности проведения сверки платежей;

(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;

(C) Раскрытие информации Платежным посредникам, Сторонним поставщикам услуг Банка и его Аффилированных лиц в связи с предоставлением Услуг;

(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;

(D) Раскрытие информации бюро кредитных историй, кредитным рейтинговым агентствам, центральным банкам и другим органам в связи с анализом рисков и принятием решений Банком, а также получение информации от них, или когда такое раскрытие информации требуется в иной связи в соответствии с действующим законодательством.

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

(E) Раскрытие информации Аффилированным лицам раскрывающей стороны и уполномоченным третьим лицам;

(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

(F) Цели, связанные с предоставлением продуктов и услуг (включая поддержку открытия счетов) Банком и его Аффилированными лицами Аффилированным лицам Клиента; и

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

(G) Любые другие цели, которые прямо разрешены другой стороной.

"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).

«**Сторонний поставщик услуг**» – третье лицо, выбираемое принимающей стороной или ее Аффилированным лицом для оказания услуг принимающей стороне или в интересах принимающей стороны, которое не является Платежным посредником (например, поставщики технологических услуг, поставщики бизнес-процессов, поставщики услуг колл-центра, поставщики аутсорсинговых услуг, внешние консультанты).

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.

3.2 Разрешенное раскрытие информации. Раскрывающая сторона соглашается (и в случаях, когда это требуется законодательством о банковской тайне или иными нормативными правовыми актами, настоящим предоставляет соответствующий отказ от осуществления права и/или соответствующее освобождение от обязательства) с тем, что принимающая сторона может использовать и раскрывать Конфиденциальную информацию раскрывающей стороны Аффилированным лицам принимающей стороны, Представителям принимающей стороны и ее Аффилированных лиц, Платежным посредникам и любым другим третьим лицам, указанным в настоящем Порядке обеспечения конфиденциальности, которым доступ к Конфиденциальной информации в разумно необходимом объеме требуется для выполнения соответствующих Разрешенных целей. Принимающая сторона обязана обеспечить, чтобы ее Аффилированные лица и Представители, которым Конфиденциальная информация раскрывающей стороны раскрывается в соответствии с настоящим п. 3.2, соблюдали конфиденциальность такой информации и использовали ее только для соответствующих Разрешенных целей.

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.

3.3 Раскрытие информации по требованию уполномоченных органов. Раскрывающая сторона соглашается (и в случаях, когда это требуется законодательством о банковской тайне или иными нормативными правовыми актами, настоящим предоставляет соответствующий отказ от осуществления права и/или соответствующее освобождение от обязательства) с тем, что принимающая сторона (а если принимающей стороной является Банк, то Банковские получатели и Платежные посредники) может (могут) раскрывать Конфиденциальную информацию раскрывающей стороны: (i) в рамках судопроизводства; (ii) в соответствии с любым регуляторным разрешением, обязательством или запросом национального или иностранного судебного и/или регулирующего органа; (iii) в соответствии с соглашением, заключенным любым из них с каким-либо национальным или иностранным государственным органом; или (iv) в соответствии с соглашением между любыми двумя или несколькими национальными или иностранными государственными органами,

включая раскрытие информации судам, трибуналам и/или юридическим, регулирующим, налоговым и другим государственным органам.

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.

4. Хранение Конфиденциальной информации.

Клиент и каждый из Банковских получателей могут хранить, использовать и при необходимости Обрабатывать Конфиденциальную информацию другой стороны в течение срока, разумно необходимого для соответствующих Разрешенных целей.

После прекращения предоставления Услуг (включая закрытие счетов) Клиент и каждый из Банковских получателей вправе хранить, использовать и при необходимости Обрабатывать Конфиденциальную информацию другой стороны в юридических и регулятивных целях, а также в целях аудита и внутреннего комплаенс-контроля, в соответствии со своим внутренним порядком архивного хранения, если это разрешается действующим законодательством и настоящим Порядком обеспечения конфиденциальности; в противном случае Клиент и каждый из Банковских получателей должны обеспечить безопасное уничтожение или удаление такой Конфиденциальной информации.

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.

5. Информационная безопасность.

Банк примет разумные и надлежащие меры физической, технической и организационной безопасности для защиты Конфиденциальной информации Клиента, находящейся в распоряжении или под контролем Банка или его Аффилированных лиц и Сторонних поставщиков услуг, от несанкционированного или неправомерного использования (или в случае Персональных данных от неправомерной Обработки), случайного уничтожения или утраты, а также примет разумные меры к обеспечению принятия таких же мер его Аффилированными лицами и Сторонними поставщиками услуг.

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

6. Персональные данные.

6.1 Термины и определения.

«**Законодательство о защите данных**» – любые применимые законы и иные нормативные правовые акты в сфере обеспечения конфиденциальности информации и защиты персональных данных, касающиеся Обработки Персональных данных, с дополнениями и изменениями.

«**Субъект данных**» означает физическое лицо, прямо или косвенно определенное или определяемое, в частности, посредством такого идентификатора, как имя, идентификационный

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.

номер, данные о местоположении, сетевой идентификатор, или одного или несколько факторов, специфичных для его физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности; либо имеет значение, установленное для этого термина или для наиболее близкого к нему термина в Законодательстве о защите данных.

"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.

«**Персональные данные**» означает любую информацию, которая может использоваться, прямо или косвенно, отдельно или в сочетании с другой информацией для идентификации Субъекта данных; либо имеет значение, установленное для этого термина или для наиболее близкого к нему термина в Законодательстве о защите данных.

"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.

«**Обработка**» означает любое действие или набор действий, выполняемых в отношении Персональных данных или наборов Персональных данных автоматизировано или без использования средств автоматизации, в том числе сбор, запись, организация, структурирование, хранение, адаптация, изменение, извлечение, консультирование, использование, раскрытие путем передачи, распространения или иным образом, выравнивание, комбинирование, ограничение, удаление, уничтожение; либо имеет значение, установленное для этого термина или для наиболее близкого к нему термина в Законодательстве о защите данных.

"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.

«**Инцидент безопасности**» – инцидент, в результате которого конфиденциальность Персональных данных раскрывающей стороны, находящихся в распоряжении или под контролем принимающей стороны, была существенно нарушена в нарушение настоящего Порядка обеспечения конфиденциальности, что создает обоснованную вероятность причинения вреда соответствующим Субъектам данных.

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.

6.2 Соответствие Законодательству о защите данных. В связи с предоставлением или получением и использованием Услуг: (i) каждая сторона обязуется соблюдать требования Законодательства о защите данных; и (ii) Клиент подтверждает, что Персональныеданные, предоставляемые им Банковским получателям, были подвергнуты Обработке добросовестно и правомерно, являются точными и релевантными для целей, в которых они предоставляются.

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'

6.3 Трансграничная передача Персональных данных. Клиент признает (и, если это требуется в соответствии с применимым законодательством, соглашается), что в связи с предоставлением Услуг и иным раскрытием информации в соответствии с п. 3 *(Разрешенное раскрытие информации)* настоящего Порядка обеспечения

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.ru/russia/main/rus/personal.htm (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

конфиденциальности Персональныеданные клиентских Субъектов данных (например, Клиента, его Аффилированных лиц, Представителей, Владельцев) могут раскрываться и/или передаваться получателям, находящимся в странах, отличных от страны, в которой действует предоставляющее Услуги учреждение Банка, или находится Клиент. При этом Банк (i) требует, чтобы его Аффилированные лица и Сторонние поставщики услугобеспечивали защиту Персональных данных в соответствии с п. 5 *(Информационная безопасность)* настоящего Порядка обеспечения конфиденциальности; и (ii) осуществляет трансграничную передачу Персональных данныхв соответствии с требованиями Законодательства о защите данных.

6.4 Правовые основания Обработки Персональных данных. В связи с Обработкой Банком Персональных данных клиентских Субъектов данных Клиент заверяет, что он (если это требуется Законодательством о защите данных) предоставил соответствующее уведомление и получил действительное согласие от Субъектов данных в связи с Обработкой Банком их Персональных данных в соответствии с настоящим Порядком обеспечения конфиденциальности, а также любыми применимыми заявлениями Банка об обеспечении конфиденциальности информации, доступными на сайте по адресу: https://www.citibank.com/tts/sa/tts-privacy-statements/index.html (или по другому URL-адресу, или в соответствии с другим заявлениями об обеспечении конфиденциальности информации, о которых Банк может уведомлять Клиента). Если Клиент сам является Субъектом данных, то Клиент заверяет (если это требуется Законодательством о защите данных), что он (a) получил указанные выше заявления об обеспечении конфиденциальности информации; и (b) дает согласие на такую Обработку.

6.5 Инциденты безопасности.

(A) Если Банку становится известно об Инциденте безопасности, то Банк проводит расследование и устраняет последствия Инцидента безопасности в соответствии со своими внутренними политиками, процедурами и требованиями применимого законодательства. Банк уведомляет Клиента об Инциденте безопасности, как только это становится практически возможным, после того, как Банку становится известно о таком Инциденте безопасности, за исключением случаев, когда на Банк налагаются соответствующие юридические или регулятивные ограничения, или когда это может помешать проводимому Банком расследованию.

(B) Каждая из сторон несет ответственность за уведомление регулирующих органов и Субъектов данных относительно Инцидента безопасности,

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.

которое требуется в соответствии с Законодательством о защите данных. Каждая сторона должна предоставить другой стороне информацию и содействие в той мере, в какой это необходимо для того, чтобы помочь другой стороне выполнить свои обязательства перед регулирующими органами и Субъектами данных.

(C) Ни одна из сторон не должна выпускать заявления для прессы или давать комментарии СМИ в связи с каким-либо Инцидентом безопасности, в которых упоминается другая сторона, если она не получила предварительного письменного разрешения другой стороны.