

Confidentiality and Data Privacy Conditions

Умови про конфіденційність та секретність даних

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

1. Вступ

Ці умови («**Умови**») визначають, яким чином кожна сторона може використовувати та повинна захищати Конфіденційну інформацію іншої сторони (включаючи персональні дані) у зв’язку з наданням Банком та отриманням і використанням Клієнтом рахунків та інших продуктів і послуг, пов’язаних чи не пов’язаних з рахунком (разом – «**Послуги**»). «**Банк**» має значення, наведене в умовах, які включають в себе ці Умови або містять посилання на них.

2. Захист конфіденційної інформації

2.1 Визначення.

«**Конфіденційна інформація**» означає інформацію (у матеріальній або нематеріальній формі), яка має відношення до сторони, яка здійснює розкриття, та/або її афілійованих осіб (включаючи будь-яку організацію, яка безпосередньо або опосередковано контролює, контролюється або перебуває під спільним контролем зі стороною), філій чи представництв (разом – «Афілійовані особи»), або їхніх відповідних Представників чи Власників, яку отримує сторона-одержувач або її Аф ілійовані особи, або їхні відповідні представники, або до якої вони мають доступ у зв’язку з наданням, отриманням чи використанням Послуг. «Конфіденційна інформація» включає в себе персональні дані, інформацію, яка має відношення до продуктів та послуг Банку, і умови, на яких вони надаються, технологію

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 (iii) a reasonable person would consider to be of a confidential and/or proprietary nature given the nature of the information and the circumstances of its disclosure.

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

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

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

2.3 Exceptions to Confidentiality.

Notwithstanding anything in these Conditions to the contrary but subject to Data Protection Law, the restrictions on the use and disclosure

(включаючи програмне забезпечення, форму і формат звітів, та екрани комп’ютера в режимі «онлайн»), інформацію про ціни, внутрішню політику, операційні процедури, реквізити банківського рахунку, інформацію про операції та будь-яку іншу інформацію, яка, у будь-якому випадку, (i) визначена стороною, яка здійснює розкриття, як конфіденційна під час розкриття, (ii) захищена відповідною банківською таємницею або іншими законами та нормами, або (iii) визначена особою в якості конфіденційної та/або приватної, враховуючи характер інформації та обставини її розкриття.

«**Власник**» означає будь-яку фізичну або юридичну особу (або її філію), яка: (i) володіє безпосередньо чи опосередковано акціями, прибутками, частками або капіталом, чи бенефіціарними частками іншої сторони, або (ii) іншим чином володіє чи здійснює контроль над стороною безпосередньо або опосередковано на правах власності, через контрольний пакет або будь-яким іншим чином, включаючи (a) особу, яка врешті решт має контрольний пакет, або яка іншим чином здійснює контроль над стороною, або (b) керівника (керівників) такої сторони.

«**Представники**» означає посадових осіб, директорів, співробітників, підрядників, агентів, представників, професійних радників сторони та постачальників послуг-третіх осіб;

2.2 Захист. Одержуюча сторона зберігатиме Конфіденційну інформацію розкриваючої сторони конфіденційною відповідно до цих правил і застосовуватиме принаймні той самий рівень захисту стосовно Конфіденційної інформації розкриваючої сторони, який одержуюча сторона застосовує для захисту власної Конфіденційної інформації аналогічного характеру, і, у будь-якому випадку, з не меншою розумною обережністю. Одержуюча сторона використовуватиме та розкриватиме Конфіденційну інформацію сторони, яка здійснює розкриття, до тієї міри, до якої це дозволено в цих Умовах.

2.3 Винятки. Незважаючи на будь-які положення цих Умов про протилежне, але за умови дотримання Закону про захист даних, обмеження на використання та розкриття

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

Конфіденційної інформації не застосовуються до: інформації, що: (i) є або стає публічною не в результаті протиправної дії чи бездіяльності одержуючої сторони або її Афілійованих осіб чи їх уповноважених Представників стосовно порушення цих Умов; (ii) є законно отриманою одержуючою стороною від третьої сторони чи вже є відомою одержуючій стороні у будь-якому випадку без повідомлення про будь-яке зобов'язання зберігати її конфіденційність; (iii) була незалежно розробленою одержуючою стороною без посилання на Конфіденційну інформацію розкриваючої сторони; (iv) було письмово погоджено уповноваженою службовою особою розкриваючої сторони, що одержуюча сторона може розкрити таку інформацію на неконфіденційній основі; чи (v) становить анонімні та/або збірні дані разом з іншою інформацією, при якій не розголошується ні Конфіденційна інформація розкриваючої сторони, ані особа будь-якого Суб'єкта даних.

3. Authorized Disclosures

3.1 Definitions.

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

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

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

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

3. Випадки дозволеного розкриття

3.1 Визначення.

«**Одержувачі Банку**» означає Банк, Афілійованих осіб банку та їхніх відповідних Представників.

«**Особа, яка сприяє платежам**» означає третю особу, яка становить частину інфраструктури платіжної системи або яка іншим чином сприяє платежам, включаючи без обмеження постачальників послуг зв'язку, клірингових та інших платіжних систем, банків-посередників, банків-агентів та банків-кореспондентів, цифрові або електронні гаманці, чи подібні організації.

«**Дозволені цілі**» означає по відношенню до використання стороною (або її Афілійованими особами, чи їхніми відповідними представниками) Конфіденційної інформації іншої сторони (або її Афілійованих осіб, чи їхніх відповідних Представників):

(A) для надання або отримання та використання Послуг згідно з їхніми відповідними умовами та для провадження відповідної діяльності, зокрема, але не виключно:

- (1) To fulfill applicable domestic and foreign legal, regulatory and compliance requirements (including know your customer (KYC) and anti-money laundering (AML) obligations applicable to a party and/or its Affiliates) and to otherwise make the disclosures specified in Condition 3.3 (Legal and regulatory disclosure);
- (2) To verify the identity or authority of a party's Representatives who interact with the other party;
- (3) For risk assessment, information security management, statistical, trend analysis and planning purposes;
- (4) To monitor and record calls and electronic communications with the other party for quality, training, investigation and fraud and other crime prevention purposes;
- (5) For fraud and other crime detection, prevention, investigation and prosecution;
- (6) To enforce and defend a party's or its Affiliates' rights; and
- (7) To manage a party's relationship with the other party (which may include the Bank providing information to the Customer and its Affiliates about the Bank's and Bank Affiliates' products and services);
- (B) To make disclosures to third parties to whose accounts the Customer instructs the Bank or Bank Affiliates to make or receive a payment from an account, or to enable such third parties to perform payment reconciliations;
- (C) To make disclosures to Payment Facilitators and to the Bank's and Bank Affiliates' Third Party Service Providers in connection with the provision of the Services;
- (D) To make disclosures to, and to obtain information from, credit information bureaus, credit rating agencies, central banks or other bodies in connection with risk-based analysis
- (1) для виконання застосовуваних вітчизняних та іноземних вимог законодавства, регуляторних норм та вимог щодо відповідності (включаючи вивчення власної клієнтури («KYC») та зобов'язання щодо боротьби з відмиванням коштів («AML»), які застосовуються до сторони та/або її Афілійованих осіб) і для здійснення іншим чином розкриття, наведеного в п. 3.3 (Юридичне та нормативне розкриття);
- (2) для верифікації особи або перевірки повноваження Представників сторони, які взаємодіють з іншою стороною;
- (3) для оцінки ризику, управління інформаційною безпекою, статистичного аналізу, аналізу трендів і в цілях планування;
- (4) для моніторингу та запису дзвінків та електронних повідомлень іншої сторони у цілях забезпечення якості, навчання, розслідування та запобігання шахрайству та іншим злочинам;
- (5) для виявлення шахрайства та інших злочинів, для запобігання їм, для їхнього розслідування та переслідування за них;
- (6) для примусового застосування та захисту прав сторони або її Афілійованих осіб, і
- (7) для управління відносинами сторони з іншою стороною (це може включати в себе надання Банком інформації Клієнту та його Афілійованим особам про продукти та послуги Банку та Афілійованих осіб Банку);
- (B) для розкриття третім особам, на рахунки яких Клієнт надає Банку або Афілійованим особам Банку вказівку здійснити або отримати платіж з рахунку або для того, щоб такі треті особи могли здійснювати звірку розрахунків;
- (C) для розкриття інформації Особам, які сприяють платежам, та Іншим постачальникам послуг як самого Банку, так і його Афілійованих осіб у зв'язку з наданням Послуг;
- (D) для розкриття інформації бюро кредитної історії, кредитним агенціям, центральним банкам або іншим органам у зв'язку з аналізом на основі оцінки ризиків та рішеннями Банку

and decisions by the Bank or where such disclosures are otherwise required by applicable law or regulation;

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

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

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

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

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

і для отримання інформації від них або у випадках, коли таке розкриття за інших обставин вимагається застосуванням законом або нормою;

(E) для розкриття інформації Афілійованим особам та визначеним нею третім особам розкриваючої сторони;

(F) у зв'язку з наданням Банком та Афілійованими особами Банку продуктів та послуг (включаючи підтримку відкриття рахунків) Афілійованим особам Клієнта, і

(G) з будь-якою додатковою метою, явним чином дозволеною іншою стороною.

«Інший постачальник послуг» означає третю сторону, доцільно обрану одержуючою стороною або її Афілійованою особою, для надання послуг одержуючій стороні або на її користь, і яка не є Постачальником платіжної інфраструктури. Приклади Інших постачальників послуг включають постачальників технічних послуг, послуг бізнес-процесу та постачальників послуг колл-центру та постачальників аутсорсингових послуг, консультантів та зовнішніх експертів

3.2 Випадки дозволеного розкриття.

Розкриваюча сторона погоджується в тому що (а у випадках, коли це вимагається застосовуваними законами про банківську таємницю або іншими застосовуваними законами, таке погодження не потребується). Одержуюча сторона може розкрити Конфіденційну інформацію розкриваючої сторони Афілійованим особам одержуючої сторони, та уповноваженим Представникам одержуючої сторони. Особам що сприяють платежам, а також будь-яким іншим особам, визначеним в цих Умовах, у яких є потреба знати таку Конфіденційну інформацію, однак тільки в обсягах, необхідних для виконання Дозволених цілей. Одержуюча Сторона гарантує забезпечити, що будь-хто з її Афілійованих осіб та Представників, яким Конфіденційна інформація Розкриваючої Сторони розкрита відповідно до цього пункту 3.2. будуть зобов'язані забезпечувати її конфіденційність та використовувати її лише для відповідних Дозволених цілей.

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 Юридичне та нормативне розкриття. Розкриваюча сторона погоджується в тому, що (а у випадках, коли це вимагається застосовуваними законами про банківську таємницю або іншими застосовуваними законами, таке погодження не потребується). одержуюча сторона (і у випадках, коли Банк є одержуючою стороною Одержувачі банку та Особи, що сприяють платежам) може розкрити Конфіденційну інформацію, якщо це вимагається відповідно до: (I) судового процесу; (II) будь-якого іншого іноземного або внутрішньодержавного юридичного та/або нормативного зобов'язання чи вимоги, (III) угоди, укладеної між будь-ким з них і будь-яким державним органом влади, внутрішньодержавним чи іноземним, (IV) або між будь-якими двома або більше внутрішньодержавними або іноземними органами влади, включаючи розкриття судам, трибуналам та/або юридичним, регулюючим, податковим та державним органам влади.

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. Період зберігання

Кожен Клієнт та Одержувач Банку має право зберігати, використовувати та (у відповідних випадках) Обробляти Конфіденційну інформацію іншої сторони протягом часу, який є обґрунтовано необхідним для досягнення відповідних Дозволених цілей. При припиненні надання Послуг (включаючи закриття Рахунків) кожному Клієнтові та усім Одержувачам Банку надається право зберігати використовувати та, якщо необхідно Обробляти Конфіденційну інформацію іншої сторони, , дотримуючись законних, нормативних, аудиторських цілей, внутрішніх цілей, а також дотримуючись внутрішньої політики управління документообігом в межах дозволених чинним законодавством, виконуючи при цьому зобов'язання передбачені цими Умовами однак в іншому випадку Конфіденційну інформацію слід знищити або видалити.

5. Information Security

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

6. Personal Data

6.1 Definitions.

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

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

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

“**Processing**” means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording,

5. Інформаційна безпека

Банк забезпечуватиме і вживатиме відповідних заходів щоб Афілійовані особи та Інші постачальники послуг забезпечували встановлення розумних і належних фізичних, технічних та організаційних заходів безпеки для захисту Конфіденційної інформації Клієнта які знаходяться в його розпорядженні або під його контролем, від несанкціонованої або незаконної Обробки(або у випадку незаконної Обробки персональних даних) та випадкового знищення чи втрати.

6. Персональні дані

6.1 Визначення.

«**Законодавство щодо захисту даних**» означає будь-які та всі застосовні закони та/чи нормативно-правові акти, що стосуються обробки Персональних даних Клієнта чи Персональних даних Банку, включаючи будь-які зміни, поправки чи доповнення до таких законів чи нормативно-правових актів,

«**Суб'єкт даних**» означає фізичну особу, ідентифіковану, або таку, що може бути ідентифікованою прямо або опосередковано, з посиланням на такі ідентифікатори як ім'я, ідентифікаційний номер, інформацію про місцезнаходження, онлайн ідентифікатори або на одну або кілька ознак фізичної, фізіологічної, психічної, генетичної, економічної, культурної та соціальної приналежності, або, у інших випадках, відповідно до чинного Законодавства щодо захисту даних.

«**Персональні дані**» означають будь-яку інформацію, що може бути використана, прямо або опосередковано, самостійно або в комбінації з іншою інформацією для ідентифікації Суб'єкта даних, або, у інших випадках, якщо інше визначення дане цьому термінові або найближчому відповідному термінові згідно з чинним Законодавством щодо захисту даних;

«**Обробка**» означає будь-яку операцію або низку операцій, які виконуються з Персональними даними або низкою Персональних даних автоматичними або неавтоматичними

organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, transfer, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, or, if different, the meaning given to this term or nearest equivalent term under Data Protection Law.

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

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

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

засобами, наприклад, збирання, запис, організація, структурування, зберігання, адаптація або зміна, повернення, консультація, використання, розкриття через передачу, поширення або забезпечення доступу в інший спосіб, регулювання або поєднання, обмеження, стирання або знищення, або, якщо інше визначення дане цьому термінові чи найближчому відповідному термінові відповідно до чинного Законодавства щодо захисту даних;

«**Інцидент інформаційної безпеки**» означає інцидент, через який конфіденційність Персональних даних розкриваючої сторони, в процесі їх зберігання або контролю одержуючою стороною, була суттєво порушена до виникнення обґрунтованого ризику заподіяння шкоди Суб’єктам персональних даних;

6.2 Дотримання Законодавства щодо захисту даних. У зв’язку з наданням або отриманням та використанням Послуг: (i) кожна сторона дотримуватиметься Законодавства щодо захисту даних та (ii) Клієнт підтверджує, що будь-які Персональні дані, які він надає Одержувачам Банку, були оброблені належним чином і законно та є точними і відповідають цілям їхнього надання.

6.3 Транскордонна передача Персональних даних. Клієнт визнає та (у тих випадках, коли це вимагається застосуванням законом або нормою) погоджується, що у зв’язку з наданням Послуг та з іншим розкриттям відповідно до пункту 3 (Випадки дозволеного розкриття) Персональні дані Суб’єктів даних Клієнта (наприклад, відповідні Представники чи Власники Афілійованих осіб) можуть бути розкриті та/або передані одержувачам, які знаходяться у країнах, які не є країною, в якій заснований Банк або його філія, що надає Послуги, або в якій знаходиться Клієнт. Проте Банк (i) вимагає від своїх Афілійованих осіб і Інших постачальників послуг здійснення захисту Персональних даних відповідно до пункту 5 (Інформаційна безпека) та (ii) здійснює транскордонну передачу Персональних даних відповідно до Законодавства щодо захисту даних.

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.citigroup.com/global/disclosures/services/treasury-and-trade-solutions-privacy-statements> (or such other URL or statement as the Bank may notify to the Customer from time to time). If the Customer is itself a Data Subject, the Customer warrants that if and to the extent required by Data Protection Law: (a) it has received the privacy disclosure(s) referenced in the preceding sentence; and (b) it consents to such Processing.

6.5 Security Incidents.

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

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

6.4 Юридичні підстави для Обробки

персональних даних. До того часу поки Банк Обробляє Персональні дані Клієнта про інших Суб'єктів даних (наприклад, персонал Клієнта чи Пов'язаних сторін), Клієнт гарантує, що в межах, необхідних відповідно до чинного законодавства, Клієнт повідомив та отримав згоду від Суб'єктів таких даних на Обробку Банком їхніх Персональних даних, згідно цих Умов та в будь-якій застосовуваній Заяві Банку про таємницю даних або в інших відомостях щодо таємниці даних, які можна знайти на <https://www.citigroup.com/global/disclosures/services/treasury-and-trade-solutions-privacy-statements> (або за такою іншою URL чи такою іншою заяву, про яку Банк може час від часу повідомити Клієнту). Якщо Клієнт сам є Суб'єктом даних, то Клієнт гарантує, що, якщо й до тієї міри, до якої це вимагається Законом про захист даних, він (а) отримав відомості про таємницю даних, згадані у попередньому реченні, та (b) згоден з такою Обробкою.

6.5 Інциденти інформаційної безпеки.

(A) Якщо Банку стає відомо про будь-який Інцидент інформаційної безпеки, Банк повинен провести розслідування та усунути наслідки такого Інциденту інформаційної безпеки відповідно до внутрішніх політики та процедур і вимог чинного законодавства. Банк повинен повідомити Клієнта про будь-який Інцидент інформаційної безпеки у найкоротші, обґрунтовано можливі строки після того, як Банку стане відомо про Інцидент інформаційної безпеки, за умови, що Банк не підлягає законодавчому обмеженню і це не поставить розслідування Банку під загрозу.

(B) Сторони погоджуються, що по відношенню до Інциденту інформаційної безпеки, кожна сторона буде зобов'язана повідомляти регулюючим органам та фізичним особам, якщо це вимагається відповідно до чинного законодавства про захист даних. Кожна сторона повинна надавати належну інформацію та допомогу іншій стороні в тій мірі, в якій це необхідно, щоб кожна сторона змогла виконати свої обов'язки перед Суб'єктами даних та регулюючими органами.

(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.

(C) Жодна сторона не повинна робити заяви чи давати коментарі в пресі та медіа стосовно Інциденту інформаційної безпеки, де згадується інша сторона, якщо на це не отримано письмову згоду іншої сторони.

Personal Data
Персональні дані