PRIVACY STATEMENT

This Privacy Statement explains how Citibank Europe plc, registered seat at Dublin, North Wall Quay 1, Ireland, registered in the Register of Companies in the Republic of Ireland, under the number 132781, conducting its business in the Czech Republic through Citibank Europe plc, organizacni slozka, registered seat at Prague 5, Stodulky, Bucharova 2641/14, Zip Code 158 02, Reg. No. 28198131, registered in the Commercial Register with the Municipal Court in Prague, Section A, Insert 59288 ("**we**", "**Citi**", "**us**", "**our**") uses or otherwise processes personal data about people with whom we come into contact (referred to as "you" in this Privacy Statement) in the course of our dealings with our clients, prospective clients (e.g. when processing personal data from a given business card) and other relevant persons. This includes employees, officers, directors, beneficial owners and other personnel or contact persons of our clients, service providers, other business counterparties or state and regulatory bodies (referred to as "client" or "Your Organization" in this Privacy Statement).

When we process your personal data, Your Organization warrants that it shall provide the information stated herein to, and shall seek any associated consent from, you. Your Organization shall also promptly, upon our request, provide evidence to us of having provided such information notice and/or obtained such consents. In connection with the foregoing, Your Organization warrants that it will provide you with a copy of this statement.

You acknowledge that Citi is entitled to send you commercial communications in connection with direct marketing of products and services similar to those provided to Your Organization.

Also, you acknowledge that you may obtain more than one version of a privacy statement, because each Citi business or function may issue and distribute its own privacy statement.

1. Who is responsible for your personal data and how can you make contact?

Citi is the controller responsible for your personal data.

For further details you may contact our Data Protection Officer at dataprotectionofficer@citi.com or Citi, 1 North Wall Quay, Dublin, D01 T8Y1, Ireland.

2. What personal data does Citi process about you?

We process personal data that you provide to us directly or that we learn about you from your use of our systems and applications and from our communications and other dealings with you and/or Your Organization. Your Organization may also give us some personal data about you. This may include:

i. **identification details** - personal data used for your unambiguous and unmistakable identification (name, surname, title, job description, date of birth, place of birth, sex, birth number, permanent address, ID number - identity card, passport or other similar document, mother's maiden name, nationality, signature; if you are a self-employed natural person, then also business name, registered office address, tax identification number and company ID);
ii. **contact details** - your business email address, personal email address, physical address and telephone number (business or personal), fax number;
iii. **transaction details** - data about executed operations, orders, telephone calls to the bank, use of a cards for payment, bank account details and other data of similar nature;
iv. other information required for KYC, AML and/or sanctions checking purposes (e.g. a copy of your passport or other relevant ID document), such as declaration if you are a politically exposed person or not, if not covered by the above categories.

Furthermore, we may also obtain personal data about you from international sanctions lists, publically available websites, databases and other public data sources.

In general, we do not process biometric data. However, from time-to-time, we may process biometric data about you that we learn from your interaction with our systems and applications. For example, in order to prevent and detect fraud, we may collect and process data about your mouse speed and movements, your keystroke rhythm or your keyboard usage characteristics, in each case in order to verify your identity. We will always provide you with additional explanatory information and any additional required disclosures if we collect and otherwise process your biometric data.

You may be able to log into or otherwise interact with our systems and applications by using biometric technology on your eligible mobile device. Such biometric authentication is a digital authentication

method that utilizes your unique biometric data (e.g. fingerprint or facial characteristics) and the built-in biometric technology on your eligible mobile device. Your biometric data remains on your eligible mobile device and is not transferred to us when this authentication method is used.

3. Why do we process your personal data?

3.1 We process your personal data, as necessary to pursue our legitimate business and other interests, for the following reasons:

a) to provide financial (banking and investment) products and services to our clients, including in connection with account opening and maintenance as well as commercial cards management, and to communicate with you and/or our clients about them;
b) for operational management, strategic planning and in order to administer, control and improve our business and client and service provider engagements;
c) for corporate marketing, business development and analysis purposes;
d) to inform other companies in the same group of companies as the client about products and services provided by us;
e) to share your identification details with insurers for the purpose of procuring an optional insurance product or automatically configured travel and accident insurance and for the performance of insurance activities related to those insurance products;
f) to monitor and analyse the use of accounts, products and services for system administration, operation, testing and support purposes;
g) to operate and manage our information technology and systems, and to ensure the security of our information technology and systems (including to detect, investigate, monitor, remediate and/or prevent security or cyber incidents);
h) to establish, exercise or defend legal claims and to protect and enforce our rights, property or safety, or to assist our clients or others to do this;
i) to investigate, respond to and address complaints or incidents relating to us or our business, to maintain service quality and to train our staff;
j) to assign or subcontract to, procure goods or services for, or outsource any part of our normal business functions to third parties;
k) to assign our receivables against a client or assign a contract between us and a client, or its part, to a third party;
l) when you or our client instruct(s) us to make a payment from an account to a third party's account, in order to enable the third party to perform payment reconciliations; and
m) for any other purpose that we specifically tell you about when we obtain personal data about you (or our client tells you about on our behalf).

3.2 We also process your personal data to comply with laws and regulations. We sometimes do more than the minimum necessary to comply with those laws and regulations, but only as necessary to pursue our legitimate interests in cooperating with our regulators and other authorities, complying with foreign laws, preventing or detecting financial and other crimes and regulatory breaches, and protecting our businesses and the integrity of the financial markets. This involves processing your personal data for the following reasons:

a) to cooperate with and respond to requests from government or regulatory bodies (such as for criminal or tax proceedings etc.), financial markets, brokers or other intermediaries or counterparties, courts, auditors or other third parties in order to comply with different laws and regulations;
b) to monitor and analyse the use of our products and services for risk assessment, planning, statistical and control purposes, including detection, prevention and investigation of fraud;
c) to conduct compliance activities such as audit and reporting, assessing and managing risk, maintenance of accounting and tax records, fraud and anti-money laundering (AML) prevention and measures relating to sanctions and anti-terrorism laws and regulations and fighting crime. This includes know your customer (KYC) screening (which involves among others identity checks and verifying address and contact details) particularly through paid databases and registers of information and commercial data (Dun & Bradstreet, World-Check, Factiva, MagnusWeb by Bisnode Česká republika a.s., Cribis by CRIF – Czech Credit Bureau, a.s., Lexis Nexis and others), Central Credit Register (established by the Czech National Bank for reciprocal

exchange of information between individual banks and branches of foreign banks on the credit burden of its clients who are legal entities or self-employed natural persons; we also provide information about loans of our clients to this register), various publicly accessible registers (such as commercial register, register of commercial activities, insolvency register etc.) or other publicly available information on the internet such as client's websites or Bloomberg, politically exposed persons screening (which involves screening client records against internal and external databases to establish connections to 'politically exposed persons' (PEPs) as part of client due diligence and onboarding) and sanctions screening (which involves the screening of clients against published sanctions lists); being a statutory requirement we also provide information about opened accounts to Central Accounts Register (established by the Czech National Bank);

d) for transaction reporting to our regulators;
e) to initiate securities or cash transfers or other instructions on behalf of Your Organization and provide confirmation of such instructions under an agreement between the client and Citi;
f) to publish data into registers of business data and report them to corresponding regulatory bodies in accordance with Regulation (EU) No. 648/2012, on OTC derivatives, central counterparties and trade repositories;
g) for declaration of beneficial ownership and tax residency.

3.3 In most cases, we do not rely on consent as the legal basis for processing your personal data. If we do rely on your consent we will make this clear to you at the time we ask for your consent.

We sometimes monitor and record selected communication, especially telephone calls. We will always notify you in advance of making such recordings. The content of this communication is confidential and we use it solely for the purpose of complying with legal obligations, concluding and fulfilling the contract with our client or Your Organization, protecting our rights and interests and, with your **consent**, for the purposes of improving customer care.

In some cases, our legal basis may be that the processing is necessary for the performance of a task carried out in the substantial public interest on the basis of law (e.g. prevention and detection of crime).

If you do not provide information that we request, we may not be able to provide (or continue providing) relevant products or services to, or otherwise do business with, you or Your Organization.

We do not process your personal data for direct marketing purposes.

4. To whom do we disclose your personal data?

Your personal data are made available to our employees in particular in connection with the performance of their employment obligations which require the handling of your personal data, only to the extent that is necessary and in compliance with all security measures.

In addition, your personal data is passed on to third parties involved in the processing of data of our clients or, where appropriate, your personal data may be made available to third parties for other reasons in accordance with the applicable laws. Prior to a transfer of your personal data to a third party, we will enter into a written agreement with that third party, in which we will outline the processing of personal data so that it contains the same guarantees for the processing of personal data that are in compliance with our legal obligations. We disclose your personal data for the reasons set out in Section 3.

4.1 We are authorized or directly obliged, without your consent, to transfer your personal data:

a) to Your Organization in connection with the products and services that we provide to it if Your Organization is our client, or otherwise in connection with our dealings with Your Organization;
b) to third parties that form part of a payment system infrastructure or which otherwise facilitate payments, including: communications, clearing and other payment systems or

similar service providers; intermediary, agent and correspondent banks; digital or ewallets; similar entities and other persons from whom we receive, or to whom we make, payments on our clients' behalf;

c) to legal, tax and other advisors or representatives, government and law enforcement authorities and other persons involved in, or contemplating, legal proceedings;
d) to competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction;
e) to collection agencies and other similar entities for the purposes of collecting our debts from our clients;
f) to other persons where disclosure is required by law or regulation or to enable products and services to be provided to you or Your Organization;
g) to prospective buyers as part of a sale, merger or other disposal of any of our business or assets;
h) to other Citi entities (this includes the entities listed at http://www.citigroup.com/citi/about/countries-and-jurisdictions/) for the purpose of managing Citi's client, service provider and other business counterparty relationships; and
i) to service providers that provide application processing, fraud monitoring, call center and/or other customer services, hosting services and other technology and business process outsourcing services.

Citi publishes on its website an up-to-date list of third parties involved in the provision of products and services by Citi at:

https://www.citibank.com/icg/sa/emea/czech/english/assets/docs/Third-Party-List.pdf

stating the appropriate purpose for the transfer to and processing of the personal data by a particular third party. The change of such third parties is regularly published by Citi. We will only pass on your personal data stated in Section 2 of this document to the extent necessary for the recipient third party.

5. Where do we transfer your personal data?

We may transfer your personal data to Citi entities, regulatory, prosecuting, tax and governmental authorities, courts and other tribunals, service providers and other business counterparties located in countries outside the European Economic Area (EEA), including countries which have different data protection standards to those which apply in the EEA. This includes transfers of personal data to India, Singapore and the United States of America.

These countries are not deemed to provide an adequate level of protection in accordance with EU (EEA) data protection laws, therefore, we have put in place European Commission-approved standard contractual clauses with the relevant third party to protect transferred personal data and for transfer of personal data within the Citigroup we use the Intra company service agreement (ICSA), General terms and conditions and ICSA Global Data Protection Addendum. These documents ensure the same level of protection guaranteed by standard contractual clauses.
Citi ensures the level of protection of personal data adequate to the level of protection guaranteed by the law of the EU (EEA) and obliges the importer of personal data to provide Citi with necessary cooperation regarding the assessment and regular re-assessment on whether the standard contractual clauses and obligations relating to ensuring sufficient safeguards and security of personal data continue to provide the level of protection of personal data adequate to the level guaranteed by the law of the EU (EEA), including taking into account the relevant aspects of the law of the third countries. You have a right to ask us for a copy of the safeguard used by contacting us as set out below.

6. How long do we keep your personal data?

We keep your personal data for as long as is necessary for the purposes for which the personal data was collected, including in connection with maintaining our relationship with you or Your Organization or for the duration of an agreement with our client or Your Organization and for the appropriate time after termination of such relationship or agreement, which may be justified in order to defend our legal claims and to protect and enforce our rights, unless otherwise required by specific law or regulation.
We are continually assessing whether it is still necessary to process certain personal data needed for a particular purpose. We also retain your personal data where necessary to enable us to comply with a legal or regulatory obligation in accordance with our records retention policies and procedures. When

the retention of your personal data is no longer necessary, we will securely destroy it, or we will irreversibly anonymize it so that it is no longer personal data.

7. Security

We protect your personal data as a bank secret and thus we process it in a manner that ensures the highest possible security preventing any unauthorized or accidental access to, change, destruction or loss of your personal data, unauthorized transmissions and other processing or misuse of your data. We comply with appropriate technical and organizational measures to ensure a level of security that meets all possible risks; all persons who come in contact with your personal data have a duty to maintain confidentiality about information obtained in connection with the processing of such data.

We will intend to pseudonymize and encrypt your personal data to the maximum extent possible if such measure is appropriate and necessary to reduce the risks arising from the processing of your personal data.

8. What are your rights in relation to your personal data?

You have the right to (i) access your personal data (ii) to correct inaccurate or untrue personal data, and (iii) to seek explanation in the event of a suspicion that the processing of personal data adversely affects the protection of your personal and private life or that your personal data are processed in contradiction with applicable law; (iv) demand the remedy of a situation that is contrary to the law, in particular by stopping personal data processing or by correction, completion or removal of your personal data, (v) erasure of your personal data if no longer necessary for the purposes for which they were collected or otherwise processed, or if it is discovered that they were processed unlawfully, (vi) restriction of the processing of personal data. You also have (vii) the right to data portability and (viii) the right to object after which the processing of your personal data will be terminated unless it can be shown that there are serious legitimate reasons for such processing which prevail over the interests or rights and freedoms of yours, in particular, if the reason is the possible enforcement of legal claims. We may ask you to verify your identity and to provide other details to help us to respond to your request.

These rights will be limited in some situations, for example, where we are required to process your personal data to comply with a legal or regulatory obligation.

To exercise these rights or if you have questions about how we process your personal data, please contact us using the contact details in Section 1. We hope that we can satisfy any queries that you may have about the way we process your personal data. We can in particular, provide copies of the data transfer safeguards referred to in Section 5. You may also complain to the relevant data protection authorities in the EEA member state where you live or work or where the alleged infringement of data protection law occurred (in the Czech Republic please contact the Office for Personal Data Protection, with registered address at Pplk. Sochora 27, Post Code 170 00, Praha 7; email: posta@uoou.cz). You can find contact information for the EEA data protection authorities here: https://edpb.europa.eu/about-edpb/board/members_en.

9. Cookies

Our web presentation accessible at https://www.citibank.com/icg/sa/emea/czech/ and https://www.citibank.com/icg/sa/emea/czech/english/ only uses cookies that are necessary to ensure that the website functions properly, for example, to maintain your session when you visit the site or to ensure that the content of the site works properly on your device. We do not use any analytics or marketing cookies or similar tracking technologies on these websites. You can find out more information here.

10. Changes to this Privacy Statement

This Privacy Statement takes effect on 25 May 2018; it was last updated on 31 January 2022. If we change it, to keep you fully aware of our processing of your personal data and related matters, we will post the new version to this website.