TTS EEA & UK COMMERCIAL CARDS PRIVACY STATEMENT

Citi's Treasury and Trade Solutions (TTS) commercial cards business provides commercial cards programs to corporations, financial institutions and public sector organizations (this Privacy Statement refers to each of these as the "**Company**"). This Privacy Statement explains how this business 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 the Company and other relevant persons. This includes individuals to whom the Company has requested Citi to issue a card ("**Cardholders**"), as well as employees, officers, directors, beneficial owners and other personnel of the Company, service providers and other business counterparties (referred to as "**Your Organization**" in this Privacy Statement).

Citi's TTS cash and trade services are governed by separate privacy statements accessible here: https://www.citibank.com/tts/sa/tts-privacy-statements/.

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

The Citi entities listed here (referred to as "we" in this Privacy Statement) are the controllers of your personal data:

- Citibank Europe plc, 1 North Wall Quay, Dublin 1, D01 T8Y1, Ireland;
- Citibank Europe plc, UK Branch, Citigroup Centre, Canada Square, Canary Wharf, London, E14 5LB, United Kingdom.

For further details you may contact our Data Protection Officer at dataprotectionofficer@citi.com or Citigroup Centre, 33 Canada Square, Canary Wharf, London E14 5LB, United Kingdom.

2. Why do we process your personal data?

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

- to provide a commercial cards program to the Company and Cardholders and to communicate with the Company and Cardholders about the program;
- to manage, administer and improve our business and Company and service provider engagements and relationships and for corporate marketing, business development and analysis purposes;
- to monitor and analyse the use of our commercial cards programs for system administration, operation, testing and support purposes;
- to operate and manage our information technology and systems, and to ensure the security of our information technology and systems;
- to establish, exercise and/or defend legal claims or rights and to protect, exercise and enforce our rights, property or safety, or to assist the Company or others to do this; and
- to investigate, respond to and address complaints or incidents relating to us or our business, to maintain service quality and to train our staff.

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:

- to cooperate with, respond to requests from, and to report transactions and/or other activity to, government, tax or regulatory bodies or other intermediaries or counterparties, courts or other third parties;
- to monitor and analyse the use of our products and services for risk assessment and control purposes (including detection, prevention and investigation of fraud);
- 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 identity checks and verifying address and contact details), 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 and their representatives against published sanctions lists); and

- to record and/or monitor telephone conversations so as to maintain service quality and security, for staff training and fraud monitoring and to deal with complaints, disputes and potential and/or actual criminal activity. To the extent permitted by law, these recordings are our sole property.

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.

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 (eg, the 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 to otherwise do business with, you or Your Organization.

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

3. Services alerts

Cardholders will automatically receive service update alerts from us by post or email where contact details have been provided to us by the Company. You will be able to opt in to receive such alerts by SMS and to receive other alerts by email by registering with CitiManager, which is a service that allows you to access and view your card statements online. Please note that, if you register for such SMS alerts, then your telecoms provider may charge you to receive such alerts if you travel abroad; we are not responsible for any such charges. If you wish to change the alerts that you receive, please do so through CitiManager or call Customer Services on the number on the back of your card.

4. Where does Citi obtain your personal data?

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 and other organisations may also give us some personal data about you, including as set out below:

- **from Your Organization:** your date of birth, nationality, title and employee ID, job description, contact details such as your business email address, home and/or business address and telephone number and other information required for KYC, AML and/or sanctions checking purposes (eg, a copy of your passport or a specimen of your signature);
- **from public sources:** information collected from international sanctions lists, publically available websites, databases and other public data sources;
- **from the Company and its program administrators:** in the case of a Cardholder, the individuals who administer the commercial cards program on behalf of the Company, and/or the Company itself, may provide personal data relating to you, and submit change of personal data requests made by you on your behalf, to us, whether through use of an electronic card management and reporting system or otherwise. Such requests may be to update any of the information about you or your account set out in your application form, such as your name, address and email address. We may contact your manager or your program administrator about you and your account; and
- **from merchants:** in the case of a Cardholder, merchants which accept our commercial cards and accounts will transfer information to the relevant bank card association and to us about any transactions that you make with them using your card or account.

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 (eg, 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.

5. To whom do we disclose your personal data?

We disclose your personal data, for the reasons set out in Section 2 above, as follows:

- to Your Organization and, if different, your employer or other members of the same group of companies, in connection with the commercial cards program that we provide to them, or otherwise in connection with our dealings with them, and authorized third parties, including, if you are a Cardholder, disclosure to program administrators and other individuals who are authorized by your Company about charges made and fees applied to your card or account, the status of your account and other data relating to your card and account, whether through use of an electronic card management and reporting system or otherwise, for the purpose of expense and travel management and administration;
- to other Citi entities (this includes the entities referenced at http://www.citigroup.com/citi/about/countrypresence/) for the purpose of managing Citi's Company, service provider and other business counterparty relationships;

- 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 your or the Company's behalf;
- to service providers who provide services which are complementary to a commercial cards program, including application processing, fraud monitoring, call center and/or other customer services, card production, hosting, and other technology and business process outsourcing services;
- to our professional service providers (eg, legal advisors, accountants, auditors, insurers and tax advisors);
- to legal advisors, government and law enforcement authorities and other persons involved in, or contemplating, legal proceedings;
- to competent regulatory, prosecuting, tax or governmental authorities, courts or other tribunals in any jurisdiction;
- to other persons, including merchants who accept our cards, where disclosure is required by law or regulation or to enable a commercial card program to be provided to you or the Company; and
- to prospective buyers as part of a sale, merger or other disposal of any of our business or assets.

6. 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) and the United Kingdom (UK), including countries which have different data protection standards to those which apply in the EEA and the UK. This includes transfers of personal data to Singapore, India and the United States of America. When we transfer your personal data to Citi entities, service providers or other business counterparties in countries outside the EEA and UK whose data protection laws are not deemed to provide an adequate level of protection, we will ensure that they protect your personal data in accordance with approved standard contractual clauses or other appropriate safeguards in accordance with EU and UK data protection laws.

7. 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 in connection with performing an agreement with the Company or Your Organization (if Your Organization is not the Company). 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 anonymise it so that it is no longer personal data.

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

You may ask us to: (i) provide you with a copy of your personal data; (ii) correct your personal data; (iii) erase your personal data; or (iv) restrict our processing of your personal data. You may also object to our processing of your personal data. 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.

Please note that the reasons for which we process your personal data are described in Section 2 above. Accordingly, if for example you ask us to erase your personal data or you ask us to restrict our processing of your personal data, this means that unfortunately we may be unable to permit you to continue to participate in our commercial cards program. Please also note that even if you ask us to erase your personal data or to restrict the processing of your personal data, we will still keep a copy of your personal data in accordance with section 7 above.

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 above. We can in particular, provide copies of the data transfer safeguards referred to in Section 6 above. You may also complain to the relevant data protection authorities in the EEA member state (or the UK) where you live or work or where the alleged infringement of data protection law occurred. You can find contact information for the EEA data protection authorities here: https://edpb.europa.eu/about-edpb/board/members_en and the UK data protection authority here: https://ico.org.uk/.

9. Changes to this Privacy Statement

This Privacy Statement takes effect on 25 May 2018; it was last updated on 21st December 2020. 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.