

Privacy Statement for Corporate – Institutional Clients and Associated Individuals

Citi provides products and services to corporations, financial institutions and public sector organizations. This Privacy Statement explains how Citi processes personal data about people with whom we come into contact (referred to as “you” in this document) in the course of our dealings with such clients and other relevant persons. This includes employees, officers, directors, legal representatives, authorized signatories, attorneys, shareholders, beneficial owners, contact persons and other personnel of our clients, service providers and other business counterparties (referred to as “Your Organization” in this document), as well as persons who deal with our clients for the execution of payment transactions (indicatively the payees).

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 document) are the controllers of your personal data: https://www.citibank.com/tts/docs/1684995_EMEA_GDPR_DataControllers.pdf

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

Any communication between you and Citibank Greece, whether oral or written, will be made in the Greek language or any other language that has been agreed with you. You may contact Citibank Greece for any queries at the telephone number +30 210 3292000 or by writing to the address 8 Othonos, 105 57 Athens.

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 financial products and services to our clients, including the execution of payment transactions and to communicate with you and/or our clients about them;
- to manage, administer and improve our business and client and service provider engagements and relationships and for corporate marketing, business development and analysis purposes;
- to monitor and analyze the use of our products and services for system administration, operation, testing and support purposes;
- to manage our information technology and to ensure the security of our 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 our clients or others to do this; and
- to investigate and respond to complaints or incidents relating to us or our business, to maintain service quality and to train staff to deal with complaints and disputes.

We also process your personal data to comply with laws and regulations. We sometimes go beyond the strict requirements of the relevant law or regulation, 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, financial markets, brokers or other intermediaries or counterparties, courts or other third parties;
- to monitor and analyze 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.

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.

3. Where does Citi obtain personal data 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 our communications and other dealings with you and/or Your Organization. Your Organization will also give us some personal data about you. This may include your date of birth, title and job description, contact details such as your business email address, physical address and telephone number and other information required for KYC, AML and/or sanctions checking purposes (eg, copies of your passport or a specimen of your signature). We also obtain some personal data about you from international sanctions lists, publically available websites, databases and other public data sources.

4. To whom do we disclose your personal data?

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

- 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;
- to other Citi entities (this includes the entities referenced at <http://www.citigroup.com/citi/about/countrypresence/>) for the purpose of managing Citi's client, service provider and other business counterparty relationships;
- to counterparty banks, payment infrastructure providers and other persons from whom we receive, or to whom we make, payments on our clients' behalf;
- to export credit agencies, multilateral agencies, development finance institutions, other financial institutions, governmental authorities and their agents, insurers, due diligence service providers and credit assessors, in each case in connection with the products and services that we provide to Your Organization if Your Organization is our client, including in connection with financings;
- 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;
- to our professional service providers (e.g., 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 where disclosure is required by law or to enable products and services to be provided to you or our clients; and
- to prospective buyers as part of a sale, merger or other disposal of any of our business or assets.

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 and the United States of America. When we transfer your personal data to Citi entities, service providers or other business counterparties in these countries, we will ensure that they protect your personal data in accordance with EEA-approved standard data transfer agreements or other appropriate safeguards.

6. How long do we keep your personal data?

We keep your personal data for as long as is necessary for the purposes of our relationship with you or Your Organization or in connection with performing an agreement with a client or Your Organization or complying with a legal or regulatory obligation and also for a prudential term reflecting the statutory limitation period (20 years).

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

You can 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 can also opt out of the processing of your personal data for direct marketing purposes or object to our other processing of your personal data. These rights will be limited in some situations; for example, where we are required to process your personal data by EU or EU member state law.

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 can in particular, provide copies of the data transfer safeguards referred to in Section 5. You can 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.

8. Changes to this Privacy Statement

This Privacy Statement takes effect on 25 May 2018; it was last updated on 25 May 2018. 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.