

Citi South Africa

Privacy Statement

This is the Privacy Statement of Citi South Africa (“Citi”). It explains how the Citi entities named below process personal information about people and organisations with whom we come into contact (referred to as “**you**” in this Privacy Statement), including our clients, service providers and other business counterparties and the individuals who represent them.

1. What is personal information?

When used in this Privacy Statement, the term “personal information” has the meaning given to it in the Protection of *Personal Information Act, 2013* (POPI). Generally speaking, personal information is any information that can be used to personally identify a natural or juristic person.

2. Who is responsible for your personal information and how can you contact them?

The Citi entities listed here (referred to as “**we**” in this Privacy Statement) are the responsible parties in respect of your personal information (depending on which entity engages with you):

- Citibank, N.A., South Africa Branch
Address: 145 West Street, Sandown, Sandton, 2196, South Africa
Telephone: +27 11 944 0000
- Citi SA Nominees Proprietary Limited
Address: 145 West Street, Sandown, Sandton, 2196, South Africa
Telephone: +27 11 944 0000
- Citigroup Global Markets Proprietary Limited
Address: 145 West Street, Sandown, Sandton, 2196, South Africa
Telephone: +27 11 944 0000
- Citigroup Global Markets Nominees Proprietary Limited
Address: 145 West Street, Sandown, Sandton, 2196, South Africa
Telephone: +27 11 944 0000

For further detail you may contact our Information Officer at informationofficerza@citi.com or by letter to the Information Officer, 145 West Street, Sandown, 2196.

Should you wish to contact the Information Regulator (South Africa), you can do so at enquiries@inforegulator.org.za.

3. Why do we process your personal information?

We process your personal information (meaning that we do things with your personal information, such as collect, store, use, share and delete), as necessary to pursue our legitimate business and other interests or to perform under a contract with you, for the following reasons:

- to provide financial products and services to our clients and to communicate with them about these products and services;
- to manage, administer and improve our business and customer and service provider engagements and relationships, for corporate marketing, business development and analysis purposes and to operate control and management information systems;
- 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, respond to and deal with complaints or incidents relating to us or our business, to maintain service quality and to train staff.

We also process your personal information in compliance with laws and regulations, including POPI and the Financial Intelligence Centre Act, 2001. 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 information 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, stock exchanges 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 general we do not process biometric information. However, from time to time, we may process biometric information about you that we learn from your interaction with our systems and applications. For example, in order to prevent and detect fraud and unusual activity and comply with our obligations under the Banks Act, 1990 to implement and maintain robust structures, policies, processes and procedures to identify customers and, in particular, recognise suspicious customers and transactions, we may use a behavioural risk detection tool which uses certain behavioural elements of biometric information to look for inconsistent or unusual user interaction with our systems and applications. We may accordingly monitor your behaviour and communications over our systems and collect and process personal information about, for example, your mouse speed and movements, your keystroke rhythm or your keyboard usage characteristics, in each case in order to verify your identity. This monitoring and interception of your communications and behavioural activity over our systems is justified under section 6 of the Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 in terms of which we are permitted to monitor such activities and communications over our systems for the purpose of detecting unauthorized use of our systems or fraudulent activity.

We may also engage a third party service provider to perform this processing and behavioural monitoring on our behalf, in which case we will ensure that such service provider is subject to appropriate data protection provisions and we will pseudo-anonymize the personal information that is provided to such service provider. If we detect unusual activity then we may notify you as such or require you to answer additional security questions to ensure that there has not been unauthorized use of our systems.

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

Save for personal information that we are required or permitted by law to collect, all personal information provided by you is provided voluntarily. However, if you do not provide information that we request, or withdraw consent previously provided, we may not be able to provide (or continue providing) relevant products or services to or otherwise do business with you or your organisation.

4. Services alerts

Holders of Citi bank cards will automatically receive service update alerts from us by post or email where contact details have been provided by them or the organisations that they represent. 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 CitiService on the number on the back of your card.

5. Where does Citi obtain personal information about you and what personal information is processed?

We process personal information 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 the organisation that

you represent. Your organisation and other organisations will also give us some personal information about you, including as set out below:

- **from the organisation which you represent:** your date of birth, nationality, title and employee ID, contact details such as your business email address, home or business address and telephone number and other information required for KYC, AML and/or sanctions checking purposes (e.g. a copy of your passport);
- **from public sources:** information collected from international sanctions lists, publically available websites, databases and other public data sources;
- **from government sources:** information collected from publically available or paid-for government sources, such as the Companies and Intellectual Property Commission;
- **from our clients and their product / service administrators:** the individuals who administer products and services, including commercial cards programs on behalf of our clients, and/or our clients themselves, may provide personal information relating to you, and submit change of personal information 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.

If the information that we obtain personally identifies you or you are reasonably identifiable from it, we will treat it as personal information.

6. To whom do we disclose your personal information?

We disclose your personal information, for the reasons set out in Section 3, as follows:

- to the organisation which you represent in connection with the products and services that we provide to it if your organisation is our client, or otherwise in connection with our dealings with your organisation;
- to your employer, other members of the same group of companies, and authorized third parties, including, if you are a cardholder, disclosure to program administrators and other individuals who are authorized by our client 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 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 your or 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 organisation if it is our client, including in connection with financings;

- to service providers who provide services which are complementary to our products and services, including application processing, fraud monitoring, call center and/or other customer services, card production 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, stock exchanges 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 to enable our 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.

We undertake never to sell your personal information.

7. Where do we transfer your personal information?

We may transfer your personal information to Citi entities, regulatory, prosecuting, tax and governmental authorities, courts and other tribunals, service providers and other business counterparties located in countries outside South Africa, including countries which have different data protection standards to those which apply in South Africa. This includes transfers of personal information to the European Economic Area, the United Kingdom, Singapore, India and the United States of America. When we transfer your personal information to Citi entities, service providers or other business counterparties in these countries, we will take all reasonable steps to ensure that they protect your personal information and that it is kept secure and receives at least a similar level of protection as that which it receives in South Africa.

8. How long do we keep your personal information?

We keep your personal information for as long as is necessary for the purposes of our relationship with you or the organisation which you represent, in connection with performing an agreement with you or your organisation or complying with a legal or regulatory obligation. Personal information is destroyed or de-identified when no longer needed or when we are no longer required by law to retain it (whichever is the later).

9. What are your rights in relation to personal information?

You have the right to contact us at any time requesting:

- (1) confirmation that we have your personal information;
- (2) access to the records containing your personal information or a description of the personal information we hold about you; and

- (3) the identity or categories of third parties who have had, or currently have, access to your personal information.

When making a request we require adequate proof of your identity, which may include providing a certified copy of your or your organisation's identity / registration documents, as may be appropriate.

We will try to provide you with suitable means of accessing information, where you are entitled to it, by for example, posting or emailing it to you.

There may be instances where we cannot grant you access to your personal information, for example, if your access would interfere with the privacy of others or would result in a breach of confidentiality, we may need to refuse access. If we refuse access, we will give written reasons for our refusal where it is practicable and legally permissible to do so.

If you believe that any personal information that we hold about you is inaccurate, irrelevant, outdated, incomplete or misleading, you may request us to correct it. If you believe that any personal information that we hold about you is excessive or has been unlawfully obtained or that we are no longer authorised to retain the information, you may request that we destroy or delete it. We will consider if the personal information requires correction, deletion or destruction and if we do not agree that there are grounds for action, you may request that we add a note to the personal information stating that you disagree with it.

We may charge a reasonable fee to cover our administrative and other reasonable costs in providing the personal information to you. We will not charge for simply making the request or for making any corrections to the personal information.

To exercise these rights or if you have questions about how we process your personal information, please contact us using the contact details in Section 2.

10. Changes to your personal information

Should your personal information change, please inform us and provide us with all changes as soon as reasonably possible to enable us to update the personal information.

11. Security and data quality

We may hold your personal information in either electronic or hard copy form. In both cases, we take reasonable and appropriate steps to ensure that the personal information is protected from misuse and loss and from unauthorised access, modification or disclosure.

12. Unlawful access to your personal information

If you believe that your personal information has been unlawfully accessed or acquired, you may contact us using the contact information above and provide details of the incident so that we can investigate it.

We will treat your complaints confidentially (unless otherwise required by law), investigate those complaints and aim to ensure that those complaints are resolved within a reasonable time.

13. Changes to this Privacy Statement

This Privacy Statement takes effect on 1 February 2019; it was last updated on 6 April 2022. If we change it, to keep you fully aware of our processing of your personal information and related matters, we will post the new version to this website and the updated version of the Privacy Statement will be effective from the date of posting.