Nedbank London Privacy Notice

Version 2/24

Introduction

This privacy notice explains how Nedbank Limited, London Branch and N.B.S.A. Limited (Nedbank) ("we", "us" or "our"), process personal data in line with, the UK General Data Protection Regulation (UK GDPR) and the UK Data Protection Act 2018. Nedbank values your privacy and is strongly committed to protecting personal data.

Where we refer to "process", it means how we use, store, make available, destroy, update, disclose, transfer or otherwise deal with personal data.

This notice is relevant to you if you are:

- an individual associated with a client or potential client of ours, such as an employee, director, officer, other representative or beneficial owner of a client; or
- an individual whose personal data is given to Nedbank by a client or potential client, or which we otherwise receive, in the course of our dealings with that client or potential client.
- an individual associated with a service provider of ours.

Who we are.

"**Nedbank London**" refers to Nedbank Limited (a company incorporated in South Africa acting through **its London Branch registered in England and Wales**, "**N.B.S.A. Limited**" refers to N.B.S.A. Limited, a company incorporated in England and Wales. Nedbank London and N.B.S.A. Limited are both part of the Nedbank Group.

How to contact us.

If you have any questions about this privacy notice for either Nedbank London or N.B.S.A. or our collection or processing of your personal data, or if you wish to exercise your data protection rights including making a complaint, our contact details are below. We are committed to working with you to obtain a fair resolution of any complaint or concerns about privacy. Please indicate which entity your query relates to so that we can respond more effectively,

Post:

Chief Compliance Officer
Nedbank Limited, London Branch
7th Floor
12 Arthur Street
London
EC4R 9AB
United Kingdom

Email: londoncompliance@nedbank.co.uk

The above contact details are also valid for N.B.S.A. Limited.

Why we collect personal data.

Personal data is any information that directly or indirectly identifies you and specifically relates to you.

We may collect and process personal data for the following purposes:

Contractual obligations: where either you receive the service or Nedbank receives the service or goods including delivery of these.

Lawful bases: when we are bound by law to collect information such as part of due diligence relating to client or supplier on-boarding, record keeping and recording and monitoring of all communication mediums including calls, instant messages, emails.

Legitimate basis: where the reason for collecting the information is assessed against our interests to ensure that these do not override your rights and protection. Such as providing your personal data to our parent in South Africa in the case of a contractor so that you can access our internal network and comply with our internal security protocols.

Consent: we will only ask for your consent to process where any of the other reasons above are not appropriate, and most importantly you have a choice to refuse.

What type of data do we collect?

It depends on the purpose we are collecting the personal data. So, depending on whether you are a supplier, or a client, the types of personal data will vary, such as:

Suppliers

Where a commercial company is providing us with a service or goods relevant to the core activity of Nedbank London or N.B.S.A., the contracting parties will need to exchange employee work related contract details or personal details as relevant to the service or goods being delivered or received.

The personal data would therefore be collected to meet the obligations under the relevant contract and consist of: Employee names, work email addresses, delivery address, work mobiles or phone numbers. Personal contact details will only be collected if necessary for the service and not formally part of the contract such as where the supplier requires their employees on Nedbank premises and/or access to Nedbank network. In these instances, Nedbank has the legitimate interest to safeguard its security measures including cyber and fraud counter measures and additional personal data will need to be collected from the Suppliers employee, such as: a copy of their passport or other form of valid Identification and security related checks (background and sanctions).

As part of our supplier due diligence, on a legal basis we may also request personal data from your employees that will be stored within a third-party provider screening tool. The additional information to the work contact details consists of: a copy of your employee's passport which contains, signature, date of birth, gender, full name, marital status and nationality.

Clients

If you're a prospective client, we will require work contact related personal data from employees, representatives, and any other individuals associated with the proposed business relationship.

Only when you have agreed to become a client of Nedbank, will we be required to collect personal data to meet the client due diligence requirements in preventing the furthering of financial crime that all financial institutions are subject to.

The personal data will consist of Know Your Client information (KYC) consisting of personal data that allows to identify and verify the identity of your:

- beneficial owner(s),
- directors,
- authorised signatories and
- other third parties associated with the business relationship.

A copy of your employee's passport will be collected which contains a sample of the employee's signature, date of birth, gender, full name, marital status and nationality.

Events

If an event is organised by us, by us in collaboration with another organisation or by a third party to which Nedbank invites you, we will only collect such personal data and other information necessary in connection with your attendance. The minimum personal information needed will be your name and that of your organisation including your job title and corporate email address so that we may keep you informed of matters relating to the event.

Depending on the event, we may also collect information about your dietary or access requirements.

Due to the nature of information requested, you will be asked for consent for collecting and processing. At any stage, you retain your right to withdraw the consent.

We may issue name badges but will not publish the list of attendees. We may need to share your information with suppliers to the event to ensure your safety (e.g. security) and that your needs are met (e.g. catering). In these situations, we will be the controller and ensure that your information is processed in accordance with our policy.

If an event organised by Nedbank, includes interactive live polls, Q&A's, this information will be collected anonymously and may be used internally within Nedbank to support further events.

Your information as provided to Nedbank will be deleted once the event has taken place.

At any time, you have a right to refuse consent or withdraw consent given even where your personal data has been collected as described further on.

How we will collect personal data about you.

We may collect personal data about you in the following manner:

- you give us the personal data:

- when filling in forms that we (or the client on our behalf) asks you to complete;
- communicating with us in person, or by email, telephone, post or otherwise.

- our systems collect the personal data about you;
- the client or your colleagues provide us with the personal data;
- third parties provide us with the personal data – these would be:
  - our service providers, agents and sub-contractors like couriers and other persons we use to offer and provide products and services;
  - Nedbank Group members, any connected companies, associates, affiliates or successors in title and/or appointed third parties (like their authorised agents, partners, contractors and suppliers);
  - other financial institutions or other credit providers in the course of a transaction relating to the client or its business;
  - On payment third party data and screening providers, and other open sources such as the internet, the media, public registers of companies;
  - attorneys, tracing agents, debt collectors and other persons that assist with the enforcement of agreements;
  - payment processing services providers, merchants, banks and other persons that assist with the processing of payment instructions from the client;
  - insurers, brokers, other financial institutions or other organisations that assist with insurance and assurance underwriting, the providing of insurance and assurance policies and products, the assessment of insurance and assurance claims and other related purposes;
  - law enforcement and fraud prevention agencies and other persons tasked with the prevention and prosecution of crime;
  - regulatory authorities, governmental departments, local and international tax authorities;
  - credit bureaux;
  - courts of law or tribunals; and
  - marketing list providers.

Recording and Monitoring

As a financial institution we are legally required to record all mediums of communications used for business purposes, which means also supplier engagements and prospective client communications. We treat this type of information as personal data.

The types of communications that we must keep a record of:

- Multiplatform messaging applications: applications that allow to share documents, video, calls or texts.
- Traditional Landlines and/or corporate mobile calls, and texts.
- Corporate emails and respective attachments.
- Traditional hard copy letters and other documents.

With the advancements in technology, you should be aware that any business-related communication channel will be recorded.

We need to record to meet our legal and regulatory obligations that require us to actively monitor our business activity to ensure that poor practices are not being carried out which can result in a determinant to you and wider society. We have strict controls limiting access to these recordings and protocols to minimise un-necessary intrusion when monitoring.

When you come and visit us.

If you come to visit us, our building has closed circuit TV systems for the security and safety of the building tenets but also the visitors.

Cookies and IP addresses

If you visit our website or that of Nedbank Group, your cookies and IP addresses and some other information such as your browser type will be recorded. *Please see our separate cookie statements on our webpages if applicable.*

How long we keep information.

The personal data detailed here will be kept for a maximum of six years or less in accordance with the lawful basis for processing the personal data and have measure in places to destructive and erase personal data in accordance with our Record Retention Schedule and Destruction Policy.

Who we share information with.

We may **disclose** personal data about you for the legitimate purposes**, to**:

- Nedbank Group companies, and specifically Nedbank Limited as Nedbank Group are our processors of personal data due to sharing the technology and security infrastructure.
- In the case of any events organised by Nedbank or to which Nedbank invites you, to suppliers of the events such as an event organiser, venue provider, security, printers and caterers.

Also closely aligned with How we collect data from you we also may share information with:

- Insurance companies
- Professional or legal advisors
- Financial and Fraud investigation authorities
- Relevant regulatory authorities
- External auditors or inspectors
- Professional consultants
- Organisations we're legally obligated to share personal data with
- Emergency services (where necessary)
- Previous employers

Transferring your personal data

Your personal data may be transferred to or in countries outside the United Kingdom, including, for example, the Republic of South Africa.

These countries may not have data protection laws as strict as those applicable in the United Kingdom. In such cases, we perform an assessment on how your rights may be affected which also requires to identify the technical organisation and security measures in place (i.e., appropriate safeguards) through a data transfer agreement so to have comfort that your personal data will be handled in accordance with UK General Data Protection (UK GDPR) and UK Data Protection Act 2018.

You may contact us for further information in this regard.

Your data protection rights.

Depending on the data protection laws that are relevant to your situation and residence, **you may have certain rights in respect of your personal data**. If you are within the scope of UK GDPR, you have the following rights:

- **Right to be informed** – the right to ask us for information about what personal data of yours is being collected and processed by us, and why it is being collected and processed;
- **Right of access** – the right obtain access to copies of your personal data;
- **Right of rectification** – the right to have your personal data corrected if it is inaccurate or incomplete;
- **Right to erasure or 'to be forgotten'** – the right to request that we erase your personal data in certain circumstances, such as when the data is no longer necessary for the purpose, the data was unlawfully processed or there are no longer lawful grounds for us to collect or process the personal data.
- **Right to restrict processing** – the right to request that we restrict the way we process your personal data. This right might be used when you contest the accuracy of your personal data, our processing is unlawful but you do not want the data erased or when we no longer need the data but you require it to establish, exercise or defend a legal claim;
- **Right to object to processing** – the right to object to processing of your personal data in circumstances where the processing is (i) based on legitimate interests, the performance of a task in the public interest or the exercise of official authority (including profiling); (ii) direct marketing (including profiling); or (iii) processing for scientific/historic research or statistic;
- **Right to data portability** – You have the right to ask that we transfer the personal data you gave us to another organisation, or to you, in certain circumstances.
- **Right to withdraw consent** – When we use consent as our lawful basis you have the right to withdraw your consent.

Please contact us if you wish to exercise any of these rights.

How to Complain

If you have any concerns about our use of your personal data, you can make a complaint to us using the contact details at the beginning of this notice.

If you remain un-satisfied with how we've used your data after raising a complaint with us, you can also complain to the ICO.

The ICO address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113

Website: https//www.ico.org.uk/make-a-complaint