NoGroup (Pty) LTD POPI POLICY 2021

Last Updated: July 2021

POLICY STATEMENT AND MANUAL OF:
PROTECTION OF PERSONAL INFORMATION AND THE RETENTION OF DOCUMENTS AND DATA
FOR
NoGroup (Pty) LTD (trading as NOSTAY)
(Registration number: 2021 / 482895 / 07)

1.1 INTRODUCTION

NOSTAY is a company functioning within the Information Technology and Software Design and Development space that is obligated to comply with The Protection of Personal Information Act 4 of 2013.

POPI requires NOSTAY to inform their clients as to the manner in which their personal information is used, disclosed, and destroyed.

NOSTAY guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The Policy sets out the manner in which NOSTAY deals with their client's personal information as well as and stipulates the purpose for which said information is used. The Policy is made available on request from NOSTAY.

The Policy is drafted in conjunction with the Financial Intermediary Association's ("FIA") Protection of Personal Information Notice.

1.2 PERSONAL INFORMATION COLLECTED

Section 9 of POPI states that "Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive."

NOSTAY collects and processes all the information and/or personal data in respect of the services being rendered in accordance with the said regulation and only for the purpose of providing the services set out in the agreement to provide services.

NOSTAY also collects and processes the client's personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

For purposes of this Policy, Clients include potential and existing clients.

1.3 TYPES OF DATA COLLECTED

While using Our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally, identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Company Registration and Vat Numbers
- Phone numbers
- Address, City, Province, Postal code

1.4 THE USAGE OF PERSONAL INFORMATION

The Client's Personal Information will only be used for the purpose for which it was collected and as agreed.

This may include:

- Providing products or services to clients and to carry out the transactions requested
- Conducting credit reference searches or- verification
- Confirming, verifying, and updating client details

- Conducting market or customer satisfaction research
- For audit and record keeping purposes
- In connection with legal proceedings
- Providing NOSTAY services to clients, to render the services requested and to maintain and constantly improve the relationship
- Providing communication in respect of NOSTAY and regulatory matters that may affect clients
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

1.5 SAFEGUARDING CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information. NOSTAY will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place in order to protect personal information:

1.5.1 NOSTAY Information Officer is Joseph Brooks whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

1.5.2 This Policy has been put in place throughout NOSTAY and training on this policy and the POPI Act has already taken place

1.5.3 Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of client and employee information, or any other action so required, in terms of POPI

1.5.4 Every employee currently employed within NOSTAY will be required to sign an addendum to their Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI

1.5.5 NOSTAY archived client information is stored in a secure location which is also governed by POPI, access is limited to these areas to authorized personal using ssh keys and only accessible via a password controlled vpn behind a firewall.

1.5.6 All electronic files and data are backed up to local and hosted servers. NOSTAY is responsible for system security that protects third party access and physical threats. NOSTAY is also responsible for Electronic Information Security.

1.6 ACCESS AND CORRECTION OF PERSONAL INFORMATION

Clients have the right to access the personal information NOSTAY holds about them. Clients also have the right to ask NOSTAY to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, NOSTAY may no longer process said personal information. NOSTAY will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

1.6.1 The details of NOSTAY's Information Officer and Head Office are as follows:

Company Name:	NoGroup (Pty) LTD
Company Tel:	087 808 5885
Company Address:	FIRST FLOOR WILLOWBRIDGE
	CARL CRONJE DRIVE
	BELLVILLE
	WESTERN CAPE
	7550
Information Officer:	Joseph Brooks
Email:	info@neuraltech.co.za
Website:	www.nostay.co.za

1.7 AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy, will take place on an ad hoc basis. Where material changes take place, clients will be notified directly, or changes will be stipulated on NOSTAY website.

1.8. RECORDS THAT CANNOT BE FOUND

If NOSTAY searches for a record and it is believed that the record either does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken the attempt to locate the record.

POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

1. PURPOSE

1.1 To exercise effective control over the retention of documents and electronic Transactions and data:
1.1.1 as prescribed by legislation and
1.1.2 as dictated by business practice.
1.2 Documents need to be retained in order to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of the Company and to minimize the Company's reputational risks.
1.3 To ensure that the Company's interests are protected and that the Company's and clients' rights to privacy and confidentiality are not breached.
1.4 Queries may be referred to the Company Secretary.

2. SCOPE & DEFINITIONS

2.1 All documents and electronic transactions generated within and/or received by the Company.

3. Definitions:

3.1 Clients includes, but are not limited to, shareholders, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.
3.2 Confidential Information refers to all information or data disclosed to or obtained by the Company by any means whatsoever.
3.3 Constitution: Constitution of the Republic of South Africa Act, 108 of 1996. 3.4 Data refers to electronic representations of information in any form.
3.5 Documents include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.
3.6 ECTA: Electronic Communications and Transactions Act, 25 of 2002.
3.7 Electronic communication refers to a communication by means of data messages.
3.8 Electronic signature refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.
3.9 Electronic transactions include e-mails sent and received.
3.10 PAIA: Promotion of Access to Information Act, 2 of 2000.

4. ACCESS TO DOCUMENTS

4.1 All Company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances (also see clause 4.2 below):
4.1.1 where disclosure is under compulsion of law
4.1.2 where there is a duty to the public to disclose
4.1.3 where the interests of the Company require disclosure and
4.1.4 where disclosure is made with the express or implied consent of the client.
4.2 Disclosure to 3rd parties:

All employees have a duty of confidentiality in relation to the Company and clients. In addition to the provisions of clause 4.1 above, the following are also applicable: 4.2.1 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of ECTA. Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.
4.2.2 Requests for company information:
4.2.2.1 These are dealt with in terms of PAIA, which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

4.2.3 Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be kept strictly confidential at all times.
4.3 The Company views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

5. STORAGE OF DOCUMENTS

5.1 HARD COPIES
5.1.1 Consumer Protection Act, No 68 of 2008
The Consumer Protection Act seeks to promote a fair, accessible and sustainable marketplace and therefore requires a retention period of 3 years for information provided to a consumer by an intermediary such as:
- Full names, physical address, postal address, and contact details
- ID number and registration number
- Contact details of public officer in case of a juristic person
- Service rendered
- Intermediary fee
- Cost to be recovered from the consumer
- Frequency of accounting to the consumer
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided
- Record of advice furnished to the consumer reflecting the basis on which the advice was given
- Written instruction sent by the intermediary to the consumer
- Conducting a promotional competition refer to Section 36(11)(b) and

5.1.2 National Credit Act, No 34 of 2005
The National Credit Act aims to promote a fair and transparent credit industry which requires the retention of certain documents for a specified period.

Retention for 3 years from the earliest of the dates of which the registrant created, signed, or received the document or from the date of termination of the agreement or in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application which applies to the documents mentioned below:

Regulation 55(1)(b):
- Records of registered activities such as an application for credit declined
- Reason for the decline of the application for credit
- Pre-agreement statements and quotes
- Documentation in support of steps taken in terms of section 81(2) of the Act
- Record of payments made
- Documentation in support of steps taken after default by consumer.
- Management accounts and financial statements.

Regulation 55(1)(d) with regard to the Credit Bureau:
- All documents relating to disputes, inclusive of but not limited to, documents from the consumer
- Documents from the entity responsible for disputed information
- Documents pertaining to the investigation of the dispute
- Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to the issues of the disputed information.

Regulation 55(1)(a) with regard to Debt Counsellors:
- Application for debt review
- Copies of all documents submitted by the consumer
- Copy of rejection letter
- Debt restructuring proposal
- Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate.

Regulation 56 with regard to section 170 of the Act:
- Application for credit
- Credit agreement entered into with the consumer.

Regulation 17(1) with regard to Credit Bureau information:
Documents with a required retention period of the earlier of 10 years or a rehabilitation order being granted:

- Sequestrations
- Administration orders.

Documents with a required retention period of 5 years:
- Rehabilitation orders
- Payment profile.

Documents with a required retention period of the earlier of 5 years or until judgment is rescinded by a court or abandoned by the credit provider in terms of section 86 of the

Magistrate's Court Act No 32 of 1944:
- Civil Court Judgments
Documents with a required retention period of 2 years:
- Enquiries.

Documents with a required retention period of 1.5 years:
- Details and results of disputes lodged by the consumers.

Documents with a required retention period of 1 year:
- Adverse information.

Documents with an unlimited required retention period:
- Liquidation.

Documents required to be retained until a clearance certificate is issued: - Debt restructuring.

5.1.3 Financial Intelligence Centre Act, No 38 of 2001:
Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below:

- Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client

- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the client's authority to act on behalf of that other person

- If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client

- The manner in which the identity of the persons referred to above was established

- The nature of that business relationship or transaction

- In the case of a transaction, the amount involved and the parties to that transaction

- All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction

- The name of the person who obtained the identity of the person transacting on behalf of the accountable institution

- Any document or copy of a document obtained by the accountable institution. These documents may also be kept in electronic format.

5.1.4 Basic Conditions of Employment Act, No 75 of 1997:
The Basic Conditions of Employment Act requires a retention period of 3 years for the documents mentioned below:

Section 29(4):
- Written particulars of an employee after termination of employment

Section 31:
- Employee's name and occupation

- Time worked by each employee

- Remuneration paid to each employee
- Date of birth of any employee under the age of 18 years.

5.2 ELECTRONIC STORAGE

We are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. We will, on an on-going basis, continue to review our security controls and related processes to ensure that your personal information remains secure.

Our security policies and procedures cover:
- Physical security
- Computer and network security
- Access to personal information
- Secure communications
- Security in contracting out activities or functions
- Retention and disposal of information
- Acceptable usage of personal information
- Governance and regulatory issues
- Monitoring access and usage of private information
- Investigating and reacting to security incidents.

When we contract with third parties, we impose appropriate security, privacy, and confidentiality obligations on them to ensure that personal information that we remain responsible for, is kept secure. We will ensure that anyone to whom we pass your personal information agrees to treat your information with the same level of protection as we are obliged to.

5.2.1 The internal procedure requires that electronic storage of information and data must be stored on a secure server and all information downloaded to an employee's computer must be removed after completion of the client's work. Data stored on the server must be adequately indexed to assist in the storage and retrieval thereof.

5.2.2 Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years must be retained for a period of 3 years after termination of employment.

5.2.3 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes, or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used. It is also required that all personal information which has become obsolete must be destroyed.

6. DESTRUCTION OF DOCUMENTS

6.1 Documents may be destroyed after the termination of the retention periods contained in this document.

6.2 NOSTAY is responsible for attending to the destruction of its client's information and data, which must be done on a regular basis.