

Protection of Personal Information Policy  
of  
Louw & Company  
"The Responsible Party"

Louw Capital Markets PTY LTD trading as Louw & Company

## 1. Version Control

The Responsible Party undertakes to review this policy regularly.

Version number	Version date	Summary of changes made
1.0 V1	July 2021	Main Policy drafted
2.0 V2	October 2023	Updates to DIO

## Contents

1.	Version Control	2
2.	Definitions	4
3.	Introduction	4
4.	Application of this Policy	4
5.	Security Measures with regards to confidentiality of personal information	4
5.1	Purpose of Collection	4
5.2	Consent	5
5.3	Information We Require	5
5.4	Access to and Integrity of Information	6
5.5	Security of Information and Regular Monitoring	6
5.6	Holding Periods	6
5.7	Information Erasure	7
5.8	Direct Marketing	7
6.	Security measures regarding an operator or person acting under authority	7
6.1	Disclosure of Information	7
6.2	Authority	7
7.	Data Breach Management	8
8.	Prohibited Data Processing and Exemptions	8
9.	Information Officer	9
10.	Deputy Information Officer	9
11.	Personal Information Transfers outside South Africa	10
12.	Prescribed Forms relating to the processing of personal information	10
13.	POPI Awareness	10
14.	Signatures	11

## 2. Definitions

**Data Subject** means the person to whom personal information relates and can be a natural or legal person.

**Personal Information** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
- Personal information concerning a child.

**Third Party Operator** means a person (natural or legal) who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

## 3. Introduction

The Protection of Personal Information Act 4 of 2013 requires that we keep plans and processes in place on how we process, store and share personal information. We respect our clients' right to privacy and endeavour to collect and use information minimally, transparently, and for the purpose for which it was collected. This Policy and supporting documents are written in easily understandable language so that it is practical and usable to a wide audience in the business.

The Responsible Party is committed to keeping information safe and secure, to provide persons with reasonable access to their information, and to give effect to the rights in terms of POPI. To this extent, we emphasise that only the necessary information is collected and used accordingly. The collection serves to protect legitimate legal interests and ensures that we are able to offer clients a service or product.

## 4. Application of this Policy

The obligations in this policy apply to The Responsible Party, its management, staff members, and representatives. Any Third Parties who The Responsible Party entrusts personal information to are also bound by the terms in this policy. It applies to all Personal Information gathered from Data Subjects.

## 5. Security Measures with regards to confidentiality of personal information

### 5.1 Purpose of Collection

The Responsible Party requires certain categories of information to ensure that clients receive high quality services and that client needs are met as they may require from time to time. The same goes for any partnerships, due diligence or other third party interactions where personal information is gathered. Information may be collected for explicitly defined purposes or incidental to the function, activity or service of the Responsible Party or a third party that might be our service providers.

The purpose of collecting information includes, but is not limited to:

- CRM: Managing and reporting on relationships with our past, present and potential clients.
- HR/Payroll: Past and present employees information is stored for HR and payroll purposes.
- Business requirements: booking trades with Strate, structuring deals, investment reporting.

The Responsible Party warrants that personal information will never be used for a reason that is not in line with what it was collected for. Should the purpose for which we collect information not be specified in this clause, the purpose will be communicated to you in writing and agreed to in our interactions with data subjects which might include varied and different parties.

## **5.2 Consent**

Any information that we collect from data subjects will be with consent. The rule of thumb is if the business is collecting information from any person whether natural or legal it must obtain a signed Consent Form. Consent may be obtained from data subjects during introductory meetings, application forms, electronic media or ongoing interaction. It might also be via online website cookies or any other form of valid consent.

Where data subjects provide us with information, the need to do so willingly and voluntarily with the understanding that we require the information to pursue both our clients' legitimate interests as well as our own.

To carry on business and to protect or facilitate data subject interests, we require personal information from time to time and will treat it with utmost confidentiality. Should a data subject at any time during the processing of their information object to the same, they may withdraw consent by furnishing us with reasonable notice and in the prescribed form attached.

## **5.3 Information we require**

The Responsible Party collects different categories of information from data subjects depending on their needs and our agreements with them. We do not collect information that is unnecessary or irrelevant for the purpose specified. We strive to collect only the information that is necessary for us to deliver our service.

To the extent that we require information from data subjects we generally collect the following information which includes but not limited to

- Name
- Job Title
- ID / Passport number
- Date of Birth
- Nationality
- Country of Residence
- Louw's opinion of the entity
- Address
- Email
- Phone
- Bank account details
- Social media urls
- Registration number
- VAT number
- Income tax number
- SARS tax pin
- BEE rating
- Annual Revenue
- FSP number
- Fund name
- Fund size
- UNESCO code
- SOR code
- CSDP details
- Portfolio manager names
- Fund administrator
- Fund management company
- Fund trustees

Please bear in mind that this is not an exhaustive list and we may at times require information that is not contained herein. We will inform data subjects as to the information we collect from them whenever practicable, whether such information is voluntary or mandatory, and what the consequences are if information (whether voluntary or mandatory) is not provided. Usually, if the information requested is not provided, we can only offer a limited service or no service at all.

## **5.4 Access to and integrity of information**

The Responsible Party is committed to maintaining the integrity and accuracy of data subject information. To this extent, data subjects are reminded via consent forms that they may request access to their own information at any time and to request that we update or correct any information that may be outdated or incorrect.

We take reasonable and routine steps to ensure that the information we collect is up to date and accurate. Where information does not need to be updated to fulfil the purpose for which it was collected, such information will not be updated without the client's express request.

The Responsible Party for the four categories of requests for access to information:

- a person requesting his or her own information;
- a person requesting information for and on behalf of another person;
- a person requesting information about another person; or
- a public body that requests information in the public interest

Requestors must provide proof of identity and a Power of Attorney, where applicable, and fill in any prescribed form as may be required from time to time. The Responsible Party may request any other information to verify the requestor's identity.

### **5.5 Security of Information and Regular Monitoring**

The safety and confidentiality of Data Subject information is of paramount importance to The Responsible Party and its staff. To this extent, The Responsible Party is committed to preventing unauthorized access, damage, loss of or destruction of personal information by ensuring that industry-appropriate and adequate security measures are implemented and persistently reviewed.

We do our best to identify risks both internally and externally, and to adapt accordingly we implement security systems with due regard to generally accepted information security practices.

The specific measures we have implemented are further elaborated on in:

- Antivirus - Bitdefender, firewall same.
- All cloud based - SSL encryption on database - SQL.
- Google workspace - backups as well stored here.
- Documents are printed but destroyed once a month, documents are placed in a secure locked bin (x2) which are collected on a monthly basis.
- 2 way encryption, VPN and VPC on all communications.

To support our security efforts, we conduct regular monitoring of our personal information security measures, which entail:

- Policy Review
- GAP Analysis Review
- File Sampling

### **5.6 Holding Periods**

Information we collect on data subjects will not be held for longer than necessary, or if the purpose for which said information was collected has ultimately been fulfilled, or if the collected information has become obsolete.

Where no agreements, other laws or terms in this policy apply, a record of personal information will be kept for one year after the information was finished being processed, including usage for the specific purpose for which the information was collected originally.

We will destroy Records of Personal Information as soon as reasonably practicable, unless further retention is required by the laws mentioned above or agreed to between the parties.

For more information on durations of specific records, please refer to Annexure A to view our Record Retainment Policy.

### **5.7 Information Erasure**

The Responsible Party will endeavour that information be destroyed, where reasonable, after its retention period has lapsed as set out in Annexure A.

Data Subjects have the right to obtain the erasure of their personal data without an undue delay if:

- the information is no longer necessary for the specified purpose it was collected for; or
- where the data subject withdraws consent in terms of this policy; or
- the collected personal information is inaccurate, irrelevant, excessive or incomplete.

If data subjects prefer for The Responsible Party to cease processing their information instead of deleting it, reasonable notice may be given to this effect following which we will immediately stop processing your information.

Notice in terms of erasure must be provided in the prescribed format of forms attached to this policy.

## 5.8 Direct Marketing

We will never process personal information for the purpose of direct marketing (or spam) unless Data Subjects:

- have consented to such processing; or
- had not previously refused consent; and if
- contact details were obtained in the context of providing them with our services; and if
- they were given reasonable opportunity to object to the direct marketing; or
- was already a data subject.
- Ensuring information policies are reviewed, monitored, up to date and sufficient.
- Ensuring an Impact Assessment is done.
- Ensuring the PAIA Manual is developed, monitored, maintained and available as prescribed. (if applicable)
- Handling complaints or requests made in term sof this policy;\Supporting this policy with relevant documentation;
- Ensuring POPI training or awareness is conducted;
- Backing up Date;
- Reporting incidents and allocating security responsibilities; and
- Any other relevant information-related duty or responsibility.

## 6. Security measures regarding an operator or person acting under authority

### 6.1 Disclosure of Information

The Responsible Party staff are regularly reminded that they have a confidentiality obligation towards data subjects who hold a Right to Privacy under the Constitution, and neither The Responsible Party nor its staff will disclose data subject information to a third party unless:

- we are required to do so by law; or
- the disclosure is necessary to enable us to perform our functions as per our clients' mandates; or
- it is vital to protecting the rights of the Responsible Party

### 6.2 Authority

In the event that information is to be disclosed to a third party, The Responsible Party will ensure that the third party receiving personal information is as committed to protecting your privacy and information as we are. We do this via obtaining a commitment form from the third party in written form where the third party agrees to keep information confidential and maintains security measures.

We disclose information to third parties such as:

- Potential and current investors are provided with confidential information of companies, for investment purposes.
- Service providers:
  - Lawyers (CDH and Hector North Attorneys)
  - Accountants (PKF)
  - Auditors (Mazars)
  - Exchanges (The Cape Town Exchange & JSE)
  - STRATE

## 7. Data Breach Management

A Data Breach incident is an event that has caused or can potentially cause damage to our organisation's assets, reputation and / or personnel which includes our customers and any other personal information we process, store or share. A Data Breach can occur

when there is intrusion, compromise and misuse of information by a party that does not have lawful access rights to the information that was compromised.

An Information Security Incident includes, but is not restricted to, the following:

- The illegitimate use of our systems for the processing, storage or sharing of data by any person.
- The transfer of personal information to persons who are not entitled to receive that information.
- The loss or theft of personal and/or classified data and information via any means, for example hacking or even attempted hacking.
- Unauthorised changes to personal information via our system hardware or software.
- Unauthorised disruption or denial of service to our system.

Where there are reasonable grounds to suspect that the personal information of a data subject has been breached (accessed, acquired, deleted or damaged by an unauthorised third party), we will:

- notify the data subject of such a breach in detail, as well as
- inform the information regulator as soon as reasonably possible after the breach is discovered.

Data breach communication to the data subject can be done in one of the following methods:

- Mailed to the data subject's last known physical or postal address;
- Sent by e-mail to the data subject's last known email address;
- Placed in a prominent position on the website of the responsible party;
- Published in the news media; or
- As may be directed by the Regulator.

The communication must include enough information so that the data subject can take protective measures and should include:

- A description of the possible consequences of the breach;
- A description of the measures that the responsible party intends to take or has taken to address the security breach;
- A recommendation with regard to the measures to be taken by the data subject
- To mitigate the possible adverse effects of the breach; and
- If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

Any data breaches experienced by Third Party Operators must be reported to the Responsible Party.

## **8. Prohibited Data Processing and Exemptions**

Due to the nature of our business we may from time to time obtain data that is prohibited to enable us to offer our services and to comply with the laws applicable to our business. As such we aim to make use of the exemptions that the POPI Act provides in instances where the information is needed. We obtain consent for this personal information and may include but not be limited to:

- The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- The criminal behaviour of a data subject to the extent that such information relates to-
  - The alleged commission by a data subject of any offence; or
  - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- Personal information concerning a child.

## **9. Information Officer**

The Responsible Party's Information Officer in terms of PAIA is tasked with:

- encouraging and ensuring compliance with PAIA;
- developing, updating and monitoring a PAIA manual for the body (that is if the organisation is required to have such a manual and does not fall under the current exemptions<sup>1</sup>); and
- assessing and providing outcomes, within the applicable time periods, to application requests which are received by the organisation, on the grounds of PAIA, to be given access to information held by the organisation.

In terms of Section 55 of POPIA, an information officer has the duty and responsibility to:

- encourage compliance by the body with the conditions for the lawful processing of personal information in terms of POPIA;
- deal with requests made to the body in terms of POPIA;
- work with the Information Regulator in relation to investigations conducted in relation to the body; and
- otherwise ensure compliance by the body with the provisions of POPIA.

Regulation 4 of the officially released Regulations Regarding the Protection of Personal Information (dated 14 December 2018), known as the POPIA Regulations, provides additional insights into the roles and obligations of an information officer. It stipulates that the information officer is accountable for ensuring:

- a compliance framework is developed, implemented, monitored, and maintained by the responsible party;
- a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- (subject to the aforementioned exemptions) a manual is developed, monitored, maintained, and made available as prescribed in terms of POPIA and PAIA;
- internal measures are developed together with adequate systems to process requests for information or access thereto; and
- internal awareness sessions are conducted regarding the provisions of POPIA.

The Responsible Party's Information Officer is Richard James Allen, with Contact Number: (066) 328 8306, and E-Mail Address: richard@louw.com.

## 10. Deputy Information Officer

The duties of a Deputy Information Officer (DIO) often align closely with those of the Information Officer (IO) in the context of data protection and information security.

The Deputy Information Officer is responsible for:

- Assist the Information Officer
- Policy Development
- Regulatory Compliance
- Security Awareness Training
- Incident Response
- Access Control
- Data Inventory
- Reporting
- Continued Education

The Responsible Party's Deputy Information Officer is Lezli Clarke, with Contact Number: (081)237 8468, and E-Mail Address: lezli@louw.com.

Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of

- such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of the Act; and
- any power or duty conferred or imposed on an information officer by this Act to a deputy information officer of that public or private body.

## 11. Personal Information Transfers outside South Africa

Due to the pervasive and widespread use of cloud technology and the disappearance of national borders in the broader context of the digital age we live in it is accepted that Personal Information of Data Subjects will almost always be transferred internationally. It is not always possible to pinpoint exactly in which country the cloud service is hosted as this may change from time to time as data centres operate internationally in several countries. It may well be the case that Personal Information is transferred to multiple countries.

The use of these services are required to be able to operate as a business, to stay competitive and to keep up to date with new digital technological innovation. We also require the use of these services to be able to provide clients with our services. For all Data Subjects we obtain consent to transfer their information across borders and this is to be done before we do so (Form 1).

The reasons or platforms we use to transfer Personal Information across borders are:

- Louw has an American minority shareholder based in the USA, with whom information is shared.
- Our cloud storage provider has physical servers that are based in either Mumbai or Sao Paulo.

## 12. Prescribed Forms relating to the processing of personal information

For Data Subjects to exercise their rights in terms of their information we need to abide by the law. In this context there are certain prescribed forms by POPI to be used when interacting with data subjects. Please see attached forms for general use.

**Form 1** - Objection to the processing of personal information -

■ FORM-1-OBJECTION-TO-THE-PROCESSING-OF-PERSONAL-INFORMATION.pdf

**Form 2** - Request for correction or deletion of personal information or destruction or deletion of record of personal information

- ■ FORM-2-REQUEST-FOR-CORRECTION-OR-DELETION-OF-PERSONAL-INFORMATION-OR.pdf

**Form 4** - Request for data subject's consent to process personal information for direct marketing -

■ FORM-4-APPLICATION-FOR-THE-CONSENT-OF-A-DATA-SUBJECT-FOR-THE-PROCESSING-OF.pdf

## 13. POPI Awareness

The responsible Party conducts POPI awareness sessions with all staff or other consultants or contractors via awareness sessions. All previously mentioned persons will be required to have completed the POPI awareness training.

From time to time more in-depth POPI awareness sessions may be held with the Information Officers and Deputy Information Officer

## 14. Signatures

As authorised signatory of the Responsible Party I, Richard James Allen hereby confirms official adoption of this policy.

**Signature:** 

**Email:** richard@louw.com

**Title:** Compliance & Administration (IO)

**Company:** Louw & Company

who warrants that I am duly authorised hereto

**Signature:** 

**Email:** andrew@louw.com

**Title:** Director

**Company:** Louw & Company









# Louw\_POPI Policy\_2023-10-20

Final Audit Report

2023-10-20

Created:	2023-10-20 (Central African Time)
By:	Team Louw (sign@louw.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAwq2y3CxstGIGEGvYO14_hcG7BUYJCms

## "Louw\_POPI Policy\_2023-10-20" History

-  Document created by Team Louw (sign@louw.com)  
2023-10-20 - 11:51:39 GMT+2
-  Document emailed to Richard Allen (richard@louw.com) for signature  
2023-10-20 - 11:52:22 GMT+2
-  Document emailed to Andrew Louw (andrew@louw.com) for signature  
2023-10-20 - 11:52:22 GMT+2
-  Email viewed by Richard Allen (richard@louw.com)  
2023-10-20 - 11:52:31 GMT+2
-  Document e-signed by Richard Allen (richard@louw.com)  
Signature Date: 2023-10-20 - 11:53:34 GMT+2 - Time Source: server
-  Email viewed by Andrew Louw (andrew@louw.com)  
2023-10-20 - 12:16:11 GMT+2
-  Document e-signed by Andrew Louw (andrew@louw.com)  
Signature Date: 2023-10-20 - 12:16:27 GMT+2 - Time Source: server
-  Agreement completed.  
2023-10-20 - 12:16:27 GMT+2