SA Tax Prac

Professional. Efficient. Affordable.

PAIA MANUAL

Prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (as amended)

DATE OF COMPILATION: 12/06/2024
DATE OF REVISION: 08/04/2026

CONTENTS OF THIS DOCUMENT

A WORD FROM THE CEO

Hi,

Thanks for taking an interest in SA Tax Prac (“SATP” for short). We’re an accounting- and tax consultancy firm in Pretoria, South Africa. As the CEO of the company, I would like to give you a better understanding of the way we do business, in the light of requirements for businesses to be transparent in their business dealings. In the digital age, we must keep documents and follow rules to protect our clients' info, which can be used for scams and fraud.

We aim to keep this manual clear, practical and easy to understand, while ensuring that it complies with the requirements of PAIA and POPIA

The bottom line of this document is.

1) This business is legally required to have it.
2) It’s also supposed to help our business stipulate how we protect people’s info

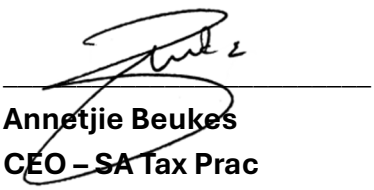
If you’re actually reading through this document, and you’re not auditor from the Regulator, I believe you’re interested in the procedure’s we’ve put in place and would like to confirm that we will make sure nobody gets access to your info without your consent of knowledge.

Kindly keep the following in mind while reading through the manual;

1) SATP is a Small Business.
   At the moment we basically employ 2 people, other than the director.
2) SATP renders services to other local Small Business.
   Our clients are not large firms or influential persons; we offer services to the businesses that may not be able to afford Deloitte or Kreston SA but still need someone to assist with their compliance with the Companies Act and at SARS.
3) SATP is also a virtual accounting firm in a big sense.
   We don’t have an office with large storage rooms, printers and lots of files with paperwork – we aim to work paperless as much as possible. Eco-friendly people.

I hope you find this manual insightful, if you have any questions, please reach out to us!

Sincerely,



Annetjie Beukes
CEO – SA Tax Prac

LIST OF THINGS YOU MAY WONDER ABOUT

"Access fee"	means a fee you may have to pay, prescribed by the Information Regulator
"CEO"	Chief Executive Officer (the boss)
"CIPC"	Companies Intellectual Property Commission
"DIO"	Deputy Information Officer (second in charge)
"FIC"	Financial Intelligence Centre (another important place like the Regulator)
"IO"	Information Officer (person who must do everything in terms of POPIA)
"PAIA"	Promotion of Access to Information Act No. 2 of 2000 (as Amended)
"POPIA"	Protection of Personal Information Act No.4 of 2013
"Regulator"	Information Regulator (the boss for the purpose of this document)
"Republic"	Republic of South Africa (our country)
"SATP"	SA Tax Prac (this firm)

WHY DO WE HAVE THIS PAIA MANUAL

PAIA helps you understand when and how we share information. This Manual is for anyone wanting to know about SATP, including:

- Who to contact to access our records.
- What records you can view without a formal PAIA request.
- How to request access to a record.
- Which laws require us to share or keep records, and how we protect your information.
- How we use your personal information and who may see it.
- The types of information we maintain.
- Whether your information might be shared outside SA and who may see it there.

Note: We don't send info overseas unless you request it. Certain regulatory bodies (SARS, FIC, Reserve Bank) operate independently. Some information may be stored on secure cloud systems outside SA.

GUIDE ON HOW TO USE PAIA

A guide has been compiled by the Information Regulator in terms of Section 10 of the Promotion of Access to Information Act, 2000, as amended. It contains information to assist people in understanding how to exercise their rights in terms of PAIA, including how to request access to records held by public and private bodies.

The guide is available in each of the official languages and may be obtained from the Information Regulator as follows:

- Website: https://www.justice.gov.za/inforeg/
- Email: enquiries@inforegulator.org.za
- Telephone: 010 023 5200

OUR CONTACT DETAILS

If you need information from us, you can contact the following persons:

Chief Information Officer

Name:	Annetjie Laura Beukes
Capacity:	Director
Designation:	Tax practitioner
Affiliations:	SAIT – General Tax Practitioner (SA)
	CIBA – Business Accountant in Practice
Cell:	071 361 9881
Email:	annetjie@sataxprac.co.za

Deputy Information Officer

No Deputy Information Officer has been appointed due to the size of the organisation. The IO fulfils all responsibilities. Queries can be escalated to the IO if no deputy exists.

Our Head Office

Physical address:	1494 Goosen street, Bergtuin Pretoria Gauteng, 0186
Postal address:	same as physical

Note that this is our registered address. If we were to have any physical paper files, it will be kept at this address – but as stated previously, we're not obligated to print anything other than the Basic Conditions of Employment Act regulations. Other stuff we keep electronically.

Contact numbers:	071 361 9881 (we don't have fax machines anymore, email works better)
Emails:	annetjie@sataxprac.co.za admin@sataxprac.co.za
Website:	www.sataxprac.co.za

HOW TO GET INFORMATION FROM US

Who can ask information about us or documents we keep?

Any person may request access to records. Any person may request access to records held by the Company in terms of PAIA. However, due to the confidential and sensitive nature of the information held, particularly financial and personal information of clients, access will be strictly assessed and may be refused in accordance with Chapter 4 of PAIA.

If you are a third-party appointed by one of our clients, we'll first confirm with them before sharing any information. Why is this? Because we work with people's financial information, which is always considered confidential and should be respected.

You can request information if:

1) The information you're looking for helps to exercise or protect any of your human rights.
2) You follow the correct procedures outlined in PAIA for requesting access to the information.
3) Access to the information is not denied based on any reasons listed in Chapter 4 of PAIA.

How to find information?

If you need information from us, please visit our website. If you can't find what you're looking for, please send us an email, or call us. It's our policy to respond within 48 hours. If you are unsure of the information you need, we'll do our best to understand what you require and how we can assist.

Will it cost anything?

Fees for access to records are prescribed in terms of the Promotion of Access to Information Act and the applicable Regulations and may be updated from time to time.
The following fees may be applicable:

- A request fee, payable when submitting a request (where applicable)
- An access fee, payable prior to access being granted to the requested records

The requester will be notified of any applicable fees and the manner of payment before the request is processed further.

May we refuse to share information?

Access to records may be refused, according to Chapter 4 of PAIA, and includes (but is not limited to):

- Protection of personal information of third parties
- Protection of confidential or commercially sensitive information
- Protection of legally privileged information
- Compliance with any other applicable legal restrictions

What to do if you did not get what you were looking for?

We may refuse access if disclosure would violate privacy, commercial confidentiality, or legal privilege. You can always contact the Information Regulator on a specific question or find their guides on their website https://inforegulator.org.za/training/wp/.

What to do if you're not happy with us?

If you find that our firm have not met the necessary requirements to protect information, or if you feel we unduly withhold information from you, kindly send a written complaint letter to the IO. If we do not respond with a workable solution, or if you are not satisfied with our feedback, you may submit a complaint to the Regulator via email at: POPIAComplaints@inforegulator.org.za or PAIAComplaints@inforegulator.org.za.

Note on Appeals: Internal appeals are only available against decisions of public bodies (like government departments). Since SA Tax Prac is a private firm, if you don't like our answer, you can complain directly to the Information Regulator.

Please refer to Annexure A for further details about information requests and Form 2.

AVAILABILITY OF OUR MANUAL

A copy of this document is available in the following two official languages, for public inspection during normal office hours:

1) English
2) Afrikaans (and for transparency's sake, it was translated by ChatGPT)

This manual is updated once a year and stored on our firm's database, as well as on our website. You can visit our website at www.sataxprac.co.za, scroll down to the bottom of any page and click the link that says "POPIA".

We're also required to send a copy to the Information Regulator, so you can always contact them as well, you can email enquiries@inforegulator.org.za or call 010 023 5200.

If you still struggle, just contact our IO at admin@sataxprac.co.za or call 071 361 9881.

TYPE OF INFORMATION WE KEEP

As a financial services company, we request the following information from our clients and store these electronically as encrypted files:

CATEGORY	DETAILS
Personal Records	- ID copies - Marital status - Selfies (photo of self, holding ID) - Tax numbers - Contact numbers and email addresses
Client Records	- Current address details - Proof of address document - Race - Language - Name of current and historic employers - Nature of remuneration (salary structure and allowances) - UIF numbers
Financial Records	- Sources of income - Bank account confirmation letters - Bank statements - Financial statements
Statutory Records	- CIPC disclosures - UBO registers - Share certificates and -registers - Special resolutions made by board

CONFIDENTIALITY DISCLOSURE

We will never share your personal information with any unauthorised party. You will always need to give permission before we share ANY information, other than information which is already available to the public.

PROCESSING OF PERSONAL INFORMATION (POPIA)

(In terms of the Protection of Personal Information Act, 4 of 2013)

Purpose of Processing Personal Information

The Company processes personal information in order to:

- Provide accounting, tax, and advisory services
- Comply with legal and regulatory obligations (including SARS, FIC, and CIPC requirements)
- Maintain client and business relationships
- Perform administrative and operational functions
- Fulfil contractual obligations

Categories of Data Subjects

The Company may process personal information relating to the following data subjects:

- Clients (individuals and juristic persons)
- Employees and prospective employees
- Service providers and suppliers
- Directors and shareholders of client entities
- Third parties authorised by clients

Categories of Personal Information

The types of personal information processed may include:

- Identification information (e.g. ID numbers, registration numbers)
- Contact details (e.g. email, telephone numbers, addresses)
- Financial information (e.g. bank statements, income details, financial records)
- Employment information
- Statutory and compliance-related information
- Any other information required to provide services or comply with legal obligations

Recipients of Personal Information

Personal information may be shared with:

- South African Revenue Service (SARS)
- Financial Intelligence Centre (FIC)
- Companies and Intellectual Property Commission (CIPC)
- Banks and financial institutions
- Professional advisors (e.g. auditors, attorneys)
- Service providers and operators who assist in delivering services
- Regulatory or governmental authorities where required by law

Cross-Border Transfers of Personal Information

The Company may store and process personal information using secure cloud-based systems and service providers. As a result, personal information may be transferred to, or stored in, countries outside of the Republic of South Africa. In such cases, the Company will ensure that

appropriate safeguards are in place to protect the information in accordance with applicable data protection laws.

Security Measures

The Company takes appropriate, reasonable technical and organisational measures to safeguard personal information, including:

- Secure electronic storage systems with restricted access
- Password protection and encryption
- Anti-virus and anti-malware protections
- Regular data backups
- Staff training on data protection and confidentiality

Data Subject Rights

Data subjects have the right to:

- Request access to their personal information
- Request correction or deletion of personal information
- Object to the processing of personal information
- Lodge a complaint with the Information Regulator

Requests can be made to the Information Officer using the contact details provided in this manual.

Retention of Records

The Company retains records of personal information in accordance with applicable legislation, including but not limited to:

- The Income Tax Act
- The Tax Administration Act
- The Companies Act
- The Financial Intelligence Centre Act

Records are generally retained for a minimum period of 5 to 7 years, or longer where required by law.

HOW WE WILL REQUEST INFORMATION

We process personal information according to applicable legal grounds, including consent, contractual necessity, and legal obligations. You are required to give us power of attorney to act on your behalf at SARS, as well as accept our appointment as your accounting officer or accountant.

We will always communicate in writing, per email or written letter. We will never request access to your bank accounts, personal pins or passwords.

Our request for information will always be from us directly, email ending with “sataxprac.co.za” and we will stipulate why we require the information, whether the information will be shared and if so, with whom.

We will never request or store information additional to what is required to do our job thoroughly.

1) When we request identification information, this is only for verification purposes and never for use other than the services you have requested.
2) If we request financial documents, like your bank statements, payslips or certificates of income from funds, this will only be for processing requirements or validation reasons.
3) Where we request any employment information or ask general questions about you personally, it would be for FICA purposes.

If we are required to share your personal information, it would be on the following grounds;

1) Your express consent or request has been made to share the information
2) We are legally obligated to share the information, and you have been informed.

Personal information may be shared where required by law, or where another lawful basis under POPIA applies.

REASONS FOR THE INFORMATION WE KEEP

We are required by law to ask and keep certain documents and information of all persons we do business with.

We don't collect documents and details just because we feel like it – we're required by law to keep certain information of everyone we do business with. Here's the breakdown:

- Financial Intelligence Centre Act (FICA): requires us to check and double-check that our clients are who they say they are. That means ID, proof of address, source of income to verify client identity and comply with anti-money laundering requirements.
- Companies Act: companies and close corporations must keep their share registers, UBOs and certain statutory records up to date. Also, financial records must be kept for at least 7 years – so we keep them on file for clients, while they also get their own copies.
- SARS laws (Income Tax Act, VAT Act, Tax Administration Act): SARS wants us to confirm IDs, tax reference numbers, and get your permission before we access your tax profile. That's why you get OTPs – not because we like bothering you.
- Basic Conditions of Employment Act: this one mostly applies internally – as an employer we must keep staff records and payroll details.
- Ethics and professional rules (SAIT & CIBA): as registered professionals, we must keep full and accurate financial info so we can prepare financial statements properly and prove we did our job with due care.
- Other laws worth a mention:
  - Electronic Communications and Transactions Act (because we work paperless and keep things online).
  - Protection of Personal Information Act (POPIA) – this one says we must handle your data carefully and only for the reasons explained here.

So, if we ask you for things like bank statements, proof of income, share certificates, or even a selfie with your ID – it's not because we're nosy. It's because one or more of the above laws say we must.

INFORMATION AVAILABLE WITHOUT PERMISSION

(Section 51(1)(c) of the Promotion of Access to Information Act, 2000)

Certain records are automatically available without the need to submit a formal request in terms of the Act. These records may be accessed through the Company's website, public platforms, or upon informal request, where applicable.

You can find the following information on our website or social media without requiring consent – these records of SATP are automatically available:

CATEGORY	**DETAILS**
General information	- Contact details - Nature of services
Demographic information	- Current address details - Language
Financial information	- None
Employment information	- Vacancies available
Statutory documents	- Registered name and registration number - PAIA Manual

These records are accessible via the Company's website at www.sataxprac.co.za or through publicly available platforms.

The Company does not make any client-related information available to the public, unless required by law or with the express consent of the data subject.

Certain information relating to registered entities may be obtained from the Companies and Intellectual Property Commission (CIPC) through its BizPortal platform.
This includes:

- Registered name
- Registration number
- Date of registration
- Registered physical- and postal address
- Names of appointed directors
- Birth date of appointed directors
- Annual Returns submitted
- Income tax reference number

The above information is not shared of our own accord but is shared by CIPC. This information is made publicly available by CIPC in terms of applicable legislation. The Company does not control the accuracy or availability of such information.

SECURITY MEASURES

You have now read a great deal about what type of company we are, type of client we service, what information we keep, why we keep it and whether or not we'll share info with the public.

It should be quite clear that we only share personal information where necessary for legal, regulatory, or operational purposes, and in accordance with applicable data protection laws.

How exactly do we ensure safety of information?
First of all, stuff is not printed out. This limits the risk of papers laying around. We aim to work paperless and keep electronic copies of documents on a designated file for each client. These files are stored on Dropbox, which is restricted by password access.

Only designated personnel have access to Dropbox and each device on which the Dropbox app is installed is noted and protected with Anti- virus and Anti-malware software. Data is not available on any other device other than the designated computers.

Our emails are connected to trusted hosting services, which ensure data is encrypted and emails not accessible by unauthorized persons.

What are our internal risk management policies?

1) Information is backed up weekly, to prevent data loss in the event of technical or cybersecurity issues.
2) Any new employees are trained on data security and protection of information, and how to navigate Dropbox to ensure data is stored in the correct format and place.
3) We actually also have an incident response plan in place. You can refer to Annexure A if you'd like to read it.

CONCLUSION

If you made it through the whole document, well done. I feel pretty impressed that I was able to draft this document myself. So, if you're an expert in POPIA and PAIA compliance, and think that there is room for improvement, you just might be right – and I would like to hear from you!

ANNEXURE A

Form 2: Request for Access to Record

(per Regulation 7 of the PAIA Regulations, 2021)

If you need access to our records, you must complete the prescribed form below ("Form 2 request for access to record"). This is the only version that will be accepted by the Information Regulator.

If you'd prefer to download it directly, here are the links:

1. Direct PDF of the form: https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-PAIA-Form02-Reg7.pdf
2. List of all PAIA forms: https://inforegulator.org.za/paia-forms/

The requester must provide sufficient detail to enable the Company to:

- Identify the record(s) requested
- Identify the requester
- Determine the form of access required

*The requester may be required to provide proof of identity to ensure that access is granted only to authorised persons.

Upon receipt of a request, we will acknowledge receipt of the request and evaluate it in accordance with PAIA. Please note that the requester may be required to pay the prescribed request fee (if applicable).

We will respond to a request within 30 (thirty) days of receipt of the request, but may extend this period by a further 30 (thirty) days if:

- The request is for a large volume of records
- Additional time is required to search for or compile the records
- Consultation with third parties is required

*The requester will be notified in writing if an extension is required.

We will inform the requester in writing if access to the requested records is granted; partially granted or if access is refused

If access is granted, the requester will be informed of any applicable access fees and the manner in which the records will be made available.

Turn to next page for FORM 2

POPIA Form 2

– page 1

ANNEXURE B

Incident Response Plan

This Incident Response Plan outlines the procedures and responsibilities for responding to and mitigating data breaches within SA Tax Prac.

Incident Identification and Reporting

All employees are responsible for promptly reporting any suspected or confirmed security incidents to the designated Incident Response Team. Incidents must be reported via email, phone, or in person to the director.

Response Procedures

Upon receiving a report of a security incident, the Incident Response Team will:

- Assess the nature and scope of the incident.
- Activate necessary resources to contain and investigate the breach.
- Implement measures to minimize further exposure or damage.
- Document all actions taken throughout the response process.

Communication and Notification

The director will be responsible for coordinating internal and external communications regarding the incident.

Depending on the severity and impact of the breach, stakeholders to be notified may include:

- Regulatory Authorities
- Affected Customers or Clients
- Law Enforcement Agencies

Legal and Compliance Considerations

A Legal Advisor will provide guidance on legal and regulatory requirements associated with the breach, including:

- Compliance with data protection laws
- Notification obligations to affected parties and regulatory authorities.
- Coordination with legal counsel for potential litigation or regulatory inquiries.

Remediation and Recovery

The director will oversee efforts to remediate vulnerabilities and restore affected systems to a secure state. Recovery measures may include:

- Patching or updating software.
- Restoring from backups.
- Implementing enhanced security controls.

Post-Incident Review and Lessons Learned

Following resolution of the incident, director will conduct a post-incident review to:

- Identify root causes and contributing factors.
- Assess the effectiveness of response efforts.
- Develop recommendations for improving incident response procedures and mitigating future risks.

Training and Awareness

Annual training and awareness programs will be conducted to educate the organisation on recognizing and responding to security incidents.

Plan Maintenance and Updates

This Incident Response Plan will be reviewed and updated annually, or as needed, to ensure its effectiveness and alignment with evolving threats and organizational changes.

By following this Incident Response Plan, SA Tax Prac aims to effectively respond to data breaches and minimize their impact on the organization and its stakeholders.