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: 01/09/2025

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.

As the CEO and IO of SA Tax Prac, I drafted this PAIA manual myself. I'm not going to give you a document that takes forever to read – because I don't want to take forever to draft it. Neither am I going to use big words to hide the fact that I'm not exactly sure what the government wants me to stipulate in the document. I'll try to make things as easy to understand as possible.

The bottom line of this document is;

1) My business is legally required to have it. I don't want to go to jail.
2) It's also supposed to help my business stipulate how I protect people's info

If you're actually reading through this document, and you're not auditor from the Regulator, I believe you're actually 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 myself.
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 has to do everything);
“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 (big-big boss for the purpose of this document); and
“Republic”	Republic of South Africa (our country)
“SATP”	SA Tax Prac (this firm)

WHY DO WE HAVE THIS PAIA MANUAL

PAIA aims to help us understand how and when to share information. This Manual may be useful to you if you are a regular John (or Jolene) wondering about the following concerning SATP:

1) Looking for the contact info for the people who can help you see the records.
2) You want to know what kinds of records we keep, that you can look at without submitting a PAIA request (formally asking).
3) Need to know how to ask for a record from us
4) What other laws say which records we must share or keep.
5) Want to know how to use this PAIA manual and where to get help.
6) Need to know if we will use your personal info, why, and who else might see it.
7) What types of information we keep.
8) Who else might see your personal info or if we might send your info out of South Africa, and who else might see it out there.
   Note, we don’t send info overseas, unless you ask us to… What SARS, FIC and the Reserve Bank does we won’t be able to control.
9) Want to know if we’re keeping your info safe and how we do that.

OUR CONTACT DETAILS

Let's address the first point – 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 one appointed (we did not deem it necessary due to the size of the firm). SATP may appoint a deputy in future. 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 numbers, this is not the 80's, email it)
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?

Let's just put one thing straight…

We know all our clients. They usually contact us personally if they need anything. So, if you're not a client and need any information on one of our clients, or of our firm, you're either going to have to be an Official Officer at SARS, the Information Regulator, an agent at the FIC, Department of Labour, attorney with mandate or a police officer with special clearance.

If you are a third-party appointed by one of our clients, I'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?

We may ask you to pay a prescribed fee, as stated in 9 Section 22(1) of PAIA. Which is R0.60 per A4 page currently.

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.

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

HOW WE WILL REQUEST INFORMATION

We will never obtain your personal information without your express consent. 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.

We will only ever share information without consent, if we are prohibited to do so by law enforcement or court order.

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 and making sure you're not secretly Osama bin Laden's cousin.
- Companies Act: companies and close corps 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 AVAILABE WITHOUT PERMISSION

You can find the following information on our website or social media without requiring consent – these records of SATP is automatically available (as prescribed in Section 52(2)):

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

Note that we do not share any information of clients on a public platform, under any circumstances. The information we keep of our clients is not required to be shared with the public.

If you register a profile with CIPC, using BizPortal, you will be able to obtain the following information about registered entities:

- 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. We take no responsibility for the information CIPC shares, only what we request from CIPC and share of our own accord.

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 that information which is already available to the public.

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 don't really share information, except where we are basically forced to do so by Government Authorities like the Information Regulator, FIC and SARS.

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/

Turn to next page for FORM 2

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

_____
_____
_____
_____
(Address)

E-mail address: _____

Fax number: _____

*Mark with an **"X"***

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request is made *(if applicable):*				
Identity Number				
Postal Address				

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (*If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)*

Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD
*(Mark the applicable box with an "**X**")*

Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "**X**")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) A request fee must be paid before the request will be considered. *b) You will be notified of the amount of the access fee to be paid.* *c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	**Facsimile**	**Electronic communication** ***(Please specify)***

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Requester / person on whose behalf request is made

---

FOR OFFICIAL USE

Reference number:	
Request received by: (State Rank, Name And Surname of Information Officer)	
Date received:	
Access fees:	
Deposit (if any):	

_____

Signature of Information Officer

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.