



APS AFRICA

CONSULT (PTY) LTD

REGISTRATION NUMBER 2016/495511/07

TAX AND ACCOUNTING:

374 Anderson Street, Menlo Park, Pretoria, 0081

AND

FIDUCIARY SERVICES:

374 Anderson Street, Menlo Park, Pretoria, 0081

AND

DATA PRIVACY TERMS AND CONDITIONS 2025



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

By providing us with your personal information, you agree to our Data Privacy Terms and Conditions, and by engaging with our business, you authorise us to process such information as set out herein.

Our Data Privacy Terms and Conditions form part of our business's overall Business Continuity Planning and apply to all external parties with whom we interact, including but not limited to individual clients, business partners, visitors to our offices, our own employees and other users of our tax advisory and accounting services. ('you').

In delivering our tax, advisory and accounting services, our business respects the privacy of your personal information, and we have implemented reasonable measures to ensure that the processing of your personal information is aligned with the requirements of the Protection of Personal Information Act 4 of 2013 ('POPIA').

In this document, we explain how and when we process personal information.

If you have questions arising from the processing of information that is not specifically listed herein, you may contact us at johanriekert@apsafrica.co.za for assistance.

Our business may review and update our Data Privacy Terms and Conditions from time to time.

1. INTRODUCTION

1. Our business specialises in the delivery of tax and accounting services.
2. In delivering these services, we deal with many role players within our business structures and in the various tax and accounting industries relative to the particular data subject and in performing our services, it is necessary to collect and process personal information as and when required, including but not limited to:
 - 2.1. Our business complying with Regulatory requirements, both in terms of the Institute for Professional Accountants and the Financial Intelligence Centre Act – amongst others;
 - 2.2. The management of client enquiries, instructions or transactions in which we act or have received instruction or are involved with in any way on a professional basis;
 - 2.3. The information required for us to attend to a matter.
 - 2.4. Some information when you browse our website or from the marketing portals on which you may have made enquiry, but we will not record any of your personal details from the website or these marketing portals unless you specifically subscribe or engage with us directly from the website or portals. These details are recorded in our website terms and conditions and in the terms and conditions on the marketing portals.
3. We may collect or obtain your personal information:
 - 3.1. Directly from you;
 - 3.2. In the course of our business relationship with you;
 - 3.3. In the course of providing our services to you;
 - 3.4. When you make your personal information public;



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- 3.5. When you visit and/or interact with our website, with us via the marketing portals or our social media platforms;
 - 3.6. When you register to access our services including but not limited to newsletters, information updates and similar services and products that we offer;
 - 3.7. When you visit our offices; and
 - 3.8. From third parties involved in your transaction.
- 3.9. We may record personal information about you such as communications and interactions with us, including, but not limited to your email and other communications with us, your details supplied for delivery of our services (such as invoicing and other such information) or at interviews in the course of applying for a job with us, subscription to our newsletters and other mailings and interactions with you during the course of digital or 'in person' marketing campaigns.
- 3.10. We treat your personal information confidentially and only use, share, record or delete it as is required by law, as part of our service delivery to you and/or as lawfully instructed by you.
- 3.11. We primarily use your personal information only for the purpose for which it was originally or primarily collected.
- 3.12. We will use your personal information for a secondary purpose only if such purpose constitutes a legitimate interest for you or for us and is closely related to the original or primary purpose for which your personal information was collected.

2. OBJECTIVE

- 2.1. Although it is not possible to ensure 100% mitigation against data breaches, the objective of our business's Data Privacy Terms and Conditions is to ensure adherence by our business and all employees associated with our business to the provisions within POPIA, together with its Regulations.
- 2.2. Our business recognises that these Regulations are aimed at protecting all of our business's data subjects from harm, ensuring that data subjects' Consent is obtained as provided for in POPIA, ensuring that data subjects' information is not unlawfully shared with third parties unless Consent for such sharing is obtained or that the sharing is lawful, stopping identity fraud, and generally protecting privacy.

3. POPIA CORE PRINCIPLES

In our quest to ensure the protection of data subjects' privacy, our business fully commits as follows:

- 3.1. To continue developing and maintaining reasonable protective measures against the possibility of risks such as loss, unauthorised access, destruction, use, alteration or revelation of personal information.
- 3.2. To regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information.
- 3.3. To ensure that the requirements of the POPIA legislation are upheld within our business. In terms of sections 8, 17 and 18 of POPIA, our business adheres to an approach of transparency of operational procedures that controls collection and processing of personal information and subscribes to a process of accountability and openness throughout its operations.

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- 3.4. In terms of the requirements set out within sections 9, 10, 11, 12, 13 14 and 15 of POPIA, our business will only collect personal information in a legal and reasonable way, for a specific reason and only if it is necessary for our operations and to process the personal information obtained from clients, employees, visitors and services suppliers only for the purpose for which it was obtained in the first place.
- 3.5. Processing of personal information obtained from clients, our employees, visitors and service suppliers will not be undertaken in an insensitive, derogative discriminatory or wrongful way that can intrude on the privacy of the particular data subject.
- 3.6. In terms of the provisions contained within sections 23 to 25 of POPIA, all our business's data subjects will be allowed to request access to certain personal information and may also request correction or deletion of personal information within the specifications of POPIA. Data subjects should refer to FORMS 1 & 2 attached hereto for these purposes.
- 3.7. Our business will not request or process information related to race, religion, medical situation, political preference, trade union membership, sexual certitude or criminal record unless this is lawfully required and unless the data subject has expressly consented. Our business will also not process information of children unless the specific consent provisions contained within POPIA have been complied with.
- 3.8. In terms of the provisions contained within section 16 of POPIA, our business continues its commitment that data subjects' information is recorded and retained accurately.
- 3.9. Our business will not provide any documentation to a third party or service provider without the express consent of the data subject except where it is necessary for the proper execution of the service as expected by the data subject.
- 3.10. Our business keeps effective record of personal information and undertakes not to retain information for a period longer than required.
- 3.11. In terms of sections 19 to 22 of POPIA, our business ensures the integrity and confidentiality of personal information in our possession and will provide the necessary security of data and keep it in accordance with prescribed legislation.

4. COLLECTION AND PROCESSING OF PERSONAL INFORMATION

We may subject your personal information to processing during the course of various activities, including:

- 4.1. The general operation of our business;
- 4.2. Analysis, evaluation, review and collation of information in order to determine potential disputes, provide project advice and preparing or commenting on opinions, project projections, responding to correspondence, reports, publications, documents relating to our projects and any other documents and records;
- 4.3. Compliance with the law and specifically fraud prevention and the combatting of money laundering;
- 4.4. Transfer of information to our service providers and operators;
- 4.5. For recruitment purposes;
- 4.6. For relationship management and marketing purposes in relation to our services (including, but not limited to, processing that is necessary for the development and improvement of our services), for accounts



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- management, and for marketing activities in order to establish, maintain and/or improve our relationship with you;
- 4.7. In addition, we may process your personal information for statistical purposes and for internal management and management reporting purposes, including but not limited to: conducting internal audits, conducting internal investigations, implementing internal business controls, providing central processing facilities, for insurance purposes and for management reporting analysis.
- 4.8. We may process your personal information for safety and security purposes.
- 4.9. We may share certain personal information with other institutions as part of our service rendering or as legally required, such as sharing information with the Receiver of Revenue, local authorities, the courts, sheriffs and the like. We only share such personal information as is required for purposes of fulfilling our service mandate or as prescribed by law.
- 4.10. Collection of personal information from another source may be necessary –
- 4.10.1. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
 - 4.10.2. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;
 - 4.10.3. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
 - 4.10.4. In the interest of national security;
 - 4.10.5. To maintain the legitimate interests of our business or of a third party to whom the information is supplied;
 - 4.10.6. Where compliance would prejudice a lawful purpose of the collection;
 - 4.10.7. Where compliance is not reasonably practicable in the circumstances of a particular contract.
- 4.11. Our business often collects personal information from other parties involved in our transactions as various professionals and property role players share clients in a single transaction.
- 4.12. Most of our communications are done electronically via the internet, per email and other electronic methods and we recognise the international risk of data and email breaches. To ensure that lawful conditions exist surrounding our data subject's information, we accept that all its South African based data subjects' Constitutional Right to Privacy is of utmost importance and that our data subjects based in other parts of the world are equally entitled to rights to privacy in terms of Regulations applicable to such data subjects in the countries in which they are based.
- 4.13. As such, we are committed to complying with South Africa's POPIA provisions, educating our data subjects about their rights to privacy, and making all necessary operational amendments.

5. CONSENT

When data subjects' information is collected, processed or shared by our business, it will be for the purposes of delivering our services. In doing so, we explain the reasons for the collection of information from the particular data subject/s and obtain the required Consent to process if the Consent is necessary and where required the sharing of the information pursuant to such explanation.



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

Our business understands the importance of obtaining our data subjects' Consent where necessary to allow our business to share information where necessary and possibly using the information for limited marketing purposes.

If personal information is used for any other reason than the original reason of it being collected, the specific Consent for such purpose will be obtained from the data subject. Our business does not use information for other purposes other than what it was collected for.

If special personal information is collected, processed and stored for any reason from any of our business's data subjects, the data subject's Consent for such collection will first be obtained.

There are instances in which the Consent to process special personal information will not be required:

- 5.1. If collection and processing are carried out with a prior consent of the data subject;
- 5.2. If collection and processing are necessary for the establishment, exercise or defence of a right or obligation in law;
- 5.3. If collection and processing are for historical, statistical or research purposes.

Our standard documentation now reflects the Consent mentioned herein and is in compliance with the POPIA.

6. STORAGE OF INFORMATION

Management and all employees of our business are aware of the risks facing data subjects regarding the storage of personal and special personal information on our business's software systems and filing copies of the physical information sheets containing personal information in our office.

To ensure that our best attempts are made to minimise data subjects from suffering loss of personal information, misuse or unauthorised alteration of information, unauthorised access or disclosure of personal information generally, we will:

- 6.1. Store personal information in databases that have built-in safeguards and firewalls to ensure the privacy and confidentiality of your information.
- 6.2. Constantly monitor the latest internet developments to ensure that the systems evolve as required. our business tests our systems regularly to ensure that our security mechanisms are up to date.
- 6.3. Continue to review our internal policies and third-party agreements where necessary to ensure that these are also complying with † POPIA and Regulations in line with our business's general Data Privacy Terms and Conditions.

7. DISPOSAL OF DATA SUBJECTS' INFORMATION

Our business is aware of its responsibility to ensure that necessary records and documents belonging to our data subjects are adequately protected and maintained and that records that are no longer needed or of no value are disposed of at the proper time and in an appropriate manner.

These rules apply to all documents and information which are collected, processed or stored by our business and include but are not limited to documents in paper and electronic format, for example, e-mail, web and text files, PDF documents etc.

In this regard, our business has developed internal policies in which we have determined when and how information and communications with and to our customers are kept and stored. The policies deal with:



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

-
- 7.1. How emails are stored and when emails are deleted destroyed;
 - 7.2. How customer data is stored, on which software systems and when these are destroyed;
 - 7.3. How physical copies of information and communications are stored and when these are destroyed.

As a matter of course, we do not discard or dispose of the telephone numbers, email addresses of data subjects and electronic communications with data subjects with whom we have previously dealt but will do so on request by the data subject.

However, since our business recognises that most of the information which it collects, processes and shares with other role players in transactions is personal of nature, we do not let information lie around and keep strict controls in respect of access to our software systems.

For this reason, we will dispose of information securely when no longer required or when requested by the data subject.

Our business acknowledges that electronic devices and media hold vast amounts of information, some of which can linger indefinitely, and we follow the following rules strictly:

- 7.4. Under no circumstances will paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse tips.
- 7.5. Our business will ensure that all electrical waste, electronic equipment and data on disk drives are physically removed and destroyed in such a way that the data will by no means be able to be virtually retrievable.
- 7.6. Our business will also ensure that all paper documents that should be disposed of are shredded locally and then recycled.
- 7.7. In the event that a third party is used for data destruction purposes, our business's Information Officer will ensure that such third party also complies with our rules and any other applicable legislation.
- 7.8. Our business may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings, and we undertake to notify employees of applicable documents where the destruction has been suspended to which they have access.
- 7.9. In the event that a document and/or information is no longer required to be stored in accordance with either legislation or in line with our own rules, it should be deleted and destroyed.
- 7.10. Our business's Information Officer will give direction where there is uncertainty regarding the retention and destruction of a document and/or information.
- 7.11. **DATA SUBJECTS ARE REFERRED TO THE ANNEXED FORMS 1 AND 2 WITH REGARD TO REQUESTS TO AMEND AND DELETE PERSONAL INFORMATION FROM OUR BUSINESS'S DATABASE.**

8. CYBER TECHNOLOGY

1. Cyber Security Culture

The repercussions of misuse of our business's systems can be severe. Potential damage includes but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage and lost productivity resulting from network downtime.



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

In order to ensure that our business's IT systems are not misused and in accordance with **ANNEXURE A**, everyone who uses or has access to our systems has received training and internal guidelines in order to meet the following five high-level IT Security requirements:

- 8.1.1. Information will be protected against any unauthorised access as far as possible;
- 8.1.2. Confidentiality of information will be assured as far as possible;
- 8.1.3. Integrity of information will be preserved as far as possible;
- 8.1.4. Availability of information for business processes will be maintained;
- 8.1.5. Compliance with applicable laws and regulations to which our business is subject will be ensured by our Information Officer as far as possible.

Every user of our IT systems is responsible for exercising good judgment regarding reasonable personal use.

2. IT Access Control

Only authorised employees may log into our business's IT system and software packages, and these are password-controlled.

All employees of our business exercise caution in allowing unauthorised access to a password, and our business's IT department ensures that passwords are reviewed and renewed from time to time—in particular where Google-based products are used and linked (such as Facebook, WhatsApp, and GMAIL-based domains).

3. Email Rules

In accordance with **ANNEXURE A**, most of our business's digital communications are conducted via email and instant messaging (IM). Given that email and IM may contain extremely sensitive and confidential information, the information involved must be appropriately protected. In addition, email and IM are potential sources of spam, social engineering attacks and malware. The misuse of email and IM can pose many legal, privacy and security risks, so it is important for users of our business's services to be aware of the appropriate use of electronic communications.

It is of use to note that all users of our business's employees are prohibited from using email to:

- 3.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
- 3.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
- 3.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
- 3.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
- 3.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
- 3.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass our business, negatively impact productivity, or harm morale.

The purpose of these rules is to ensure that information sent or received via our business's IT systems is appropriately protected, that these systems do not introduce undue security risks to our business and that users are made aware of what our business deems as acceptable and unacceptable use of its email and IM.

4. Our business's rules related to handheld devices



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

Many users of technology fail to recognise that mobile devices represent a threat to IT and data security. As a result, technology users often do not apply the same level of security and data protection as they would on other devices such as desktop or laptop computers.

Our business safeguards the physical and data security of mobile devices such as smartphones, tablets, and other mobile devices like PC's and Notebooks and our business's Information Officer and the IT department ensure that:

- 4.1. Our business's users of handheld devices diligently protect their devices from loss and disclosure of private information belonging to or maintained by our business and that this is achieved with constant awareness training.
- 4.2. Before connecting a mobile handheld device to the network at our business, users are expected to ensure it is on the list of approved devices issued by IT support wherever necessary.
- 4.3. In the event of a security incident or if suspicion exists that the security of our business's systems has been breached, the person in our business who becomes aware of the breach shall notify the IT support team immediately together with our business's Information Officer especially when a mobile device may have been lost or stolen.

5. Anti-virus rules

- 5.1. Management of our business is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into our business's programs (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited.
- 5.2. Our business's employees are discouraged from attempting to remove viruses themselves. If a virus infection is detected, users are expected to disconnect from our business's networks, stop using the infected computer immediately and notify the IT support.
- 5.3. Our business has contracted with appropriate anti-virus software in order to protect all digital platforms and devices. A summary of the anti-virus measures can be found in **ANNEXURE A**.

It is further worth noting that our business's users are encouraged to be cautious of e-mail attachments from an unknown source as viruses are often hidden in attachments.

All employees have received and will continue to receive internal training in respect of such viruses and how to identify them and what to do if a virus is suspected.

6. Physical access control

All of our business's premises, which include computers and other types of information technology resources, will be safeguarded against unlawful and unauthorised physical intrusion, as well as fire, flood and other physical threats. Our business has also implemented a **BUSINESS CONTINUITY PLAN** in which all risks and crises are mitigated and processes in respect to these crises and risks (including cyber risks) are contained.

2. THIRD PARTY OPERATORS

In order for our business to deliver our services efficiently, it is necessary at times to share data subjects' personal and special personal information with third parties for specific reasons related to our service delivery. As referenced in clauses 1 to 5 above, where necessary we will obtain the necessary Consent when required from the particular data subject.



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

Where data subjects' information is shared with these third-party operators, our business enters into **OPERATORS' AGREEMENT** with the relevant third-party where possible.

These **OPERATORS' AGREEMENTS** are necessary in order to ensure that the third-party operator treats the personal information of our data subjects responsibly and in accordance with the provisions contained in the POPI Act and Regulations thereto. When we present our **OPERATORS' AGREEMENTS** to a third-party for signature, we usually request copies of the third-party operators' POPIA Policy, rules, internet rules and details of the third-party's Information Officer.

3. BANKING DETAILS

It is a known fact that South African businesses are particular targets for email interceptions and in particular the interception of banking details for purposes of payment in respect of transactions. Our data subjects are open to large amounts of damages and losses if emails are intercepted, and banking details are fraudulently amended without the data subject's knowledge.

We have implemented a **PAYMENT POLICY** in accordance with which our employees are formally held liable when not following our rules as well as clear warnings within all our correspondences (emails and physical letters) warning data subjects of the risks of email hacking and interceptions. In the event that banking details are sent to data subjects or received from data subjects for purposes of payment, the banking details will be sent via a secure channel (other than email) and must be confirmed with a telephone call and a follow up WhatsApp. It is recorded that, in certain instances, data subjects' bank details are to be shared with relevant third parties but in such event, all care shall be taken to ensure encryption of emails.

4. DIRECT MARKETING

Our business does not share data subjects' information with third parties for the sole purpose of such third-party marketing to our data subjects. In the event that any associated third-party using the data subjects' information it collected from our business, our business takes no responsibility for any consequences suffered by the data subject which may have been caused by the third-party's actions.

Our business does not send out bulk emails to our database of existing clients. In the event that our business adopts a new direct marketing strategy in which we start sending out these bulk emails, we will ensure that the required **OPTING OUT/UNSUBSCRIBE** options, which allow the recipients of the emails to request removal of their details from these bulk emails are clearly implemented.

5. DATA CLASSIFICATION

In accordance with our business's internal policies all of our business's employees share in the responsibility for ensuring that our information assets receive an appropriate level of protection as set out hereunder:

- 5.1. Our managers are responsible for assigning classifications to information assets according to the standard information classification system presented below.
- 5.2. Where practicable, the information category shall be embedded in the information itself.
- 5.3. All employees of our business shall be guided by the information category in their security-related handling of our information. All information entrusted to us from third parties falls into one of three classifications in the table below, presented in order of increasing sensitivity.



APS Africa Consult (Pty) Ltd
 REGISTRATION NUMBER 2016/495511/07
 Tel: 012 8832069 / www.aps-africa.com

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
 DATA PRIVACY TERMS AND CONDITIONS
 2024**

Information Description	Examples	Category
Unclassified Public	Information is not confidential and can be made public without any implications for our business	Product brochures widely distributed Information widely available in the public domain, including publicly available website areas. Financial reports required by regulatory authorities. Newsletters for external transmission
Proprietary	Information is restricted to management, approved internal access and protected from external access. Unauthorised access could influence our business's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	Passwords and information on corporate security procedures. Know-how used to process client information. Standard Operating Procedures are used in all parts of our business's activities. All software codes developed by our business whether used internally or sold to clients.
Client Confidential Data	Information collected and used by our business in the conduct of its business to employ people, to log and fulfil client mandates, and to manage all aspects of corporate finance. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	Salaries and other personnel data. Accounting data and internal financial reports Confidential customer business data and confidential contracts. Non-disclosure agreements with clients/ vendors Company business plans.

13. RIGHTS OF THE DATA SUBJECT- FORMS 1 & 2 ATTACHED

- 13.1. All of our data subjects or competent persons where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing that the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information is not affected.
- 13.2. Any of our data subjects may object, at any time, to the processing of personal information–
 - 13.2.1. In writing, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
 - 13.2.2. For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.
- 13.3. All of our data subjects, having provided adequate proof of identity, have the right to–



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- 13.3.1. Request from us to confirm, free of charge, whether we hold personal information about the data subject; and
- 13.3.2. Request from our business a record or a description of the personal information about the data subject held by us including information about the identity of all third-parties, or categories of third-parties, who have, or have had, access to the information – within a reasonable time; at a prescribed fee as determined by our business's Information Officer; in a reasonable manner and format; and in a form that is generally understandable.
- 13.4. Our data subjects may, in the prescribed manner, request our business to –
 - 13.4.1. correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or
 - 13.4.2. destroy or delete a record of personal information about the data subject that our business is no longer authorised to retain.
- 13.5. Upon receipt of a request referred to in clause 13.4, our business will, as soon as reasonably practicable –
 - 13.5.1. correct the information;
 - 13.5.2. destroy or delete the information;
 - 13.5.3. provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or
 - 13.5.4. where an agreement cannot be reached between our business and the data subject, and
 - 13.5.5. if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.
- 13.6. our business will inform the data subject, who made a request as set out in clause 13.5 of the action taken as a result of the request.

14. INFORMATION OFFICER

Appointed Information Officer:

INFORMATION OFFICER: JOHAN RIEKERT

Contact details +27 (0)12 001 8793

Postal Address: 374 Anderson Street, Menlo Park, Pretoria, 0081

Street Address: 374 Anderson Street, Menlo Park, Pretoria, 0081

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

14.1. The general responsibilities of our business's Information Officer include the following:

- 14.1.1. The encouragement of compliance, by all employees with the conditions for the lawful processing of personal information;
- 14.1.2. Managing requests made to our business pursuant to POPIA and PAIA;
- 14.1.3. Working with the Regulator in relation to investigations conducted pursuant to prior authorisation required to process certain information of POPIA in relation to the firm.
- 14.1.4. Continuously perform data backups, store at least weekly backup offsite, and test those backups regularly for data integrity and reliability.
- 14.1.5. Review policy rules regularly, document the results, and update the policy as needed.
- 14.1.6. Continuously update information security policies and network diagrams.
- 14.1.7. Secure critical applications and data by patching known vulnerabilities with the latest fixes or software updates.
- 14.1.8. Perform continuous computer vulnerability assessments and audits.

14.2. The data breach responsibilities of our business's Information Officer include the following:

- 14.2.1. Ascertain whether personal data was breached;
- 14.2.2. Assess the scope and impact by referring to the following:
 - 14.2.2.1. Estimated number of data subjects whose personal data was possibly breached
 - 14.2.2.2. Determine the possible types of personal data that were breached
 - 14.2.2.3. List security measures that were already in place to prevent the breach from happening.
- 14.2.3. Once the risk of the breach is determined, the following parties need to be notified within 72 hours after being discovered:
 - 14.2.3.1. The Information Regulator
 - 14.2.3.2. Communication should include the following:
 - 14.2.3.2.1. Contact details of Information Officer
 - 14.2.3.2.2. Details of the breach,
 - 14.2.3.2.3. Likely impact,
 - 14.2.3.2.4. Actions already in place, and those being initiated to minimise the impact of the data breach.
 - 14.2.3.2.5. Any further impact is being investigated (if required), and necessary actions to mitigate the impact are being taken.

14.3. Review and monitor

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- 14.3.1. Once the personal data breach has been contained, our business will conduct a review of existing measures in place and explore the possible ways in which these measures can be strengthened to prevent a similar breach from reoccurring.
- 14.3.2. All such identified measures should be monitored to ensure that the measures are satisfactorily implemented.

15. FINANCIAL INTELLIGENCE CENTRE ACT

- 15.1. Due to International pressures, the South African FINANCIAL INTELLIGENCE CENTRE has vastly amended its anti-corruption, anti-money laundering and anti-terrorism laws and expanded the list of industries that must now apply FICA to their transactions.
- 15.2. All operations of our business are now subjected to these new FICA rules and all our clients are required to undergo the new FICA processes. These processes oblige our business to collect in-depth personal and often special personal information from our clients and assess this information internally. Some information which our business collects may be shared with the FIC from time to time.
- 15.3. The FIC Act clarifies the issue of data privacy of client information for our business who will often be collecting, verifying and screening client information without a specific consent form such client. The processing of personal and special personal information of clients for the purposes of the FIC Act compliance may only be done within the confines of the POPI Act.
- 15.4. While the processing and further processing of personal information of a client for purposes of FIC Act requirements is allowed in terms of the POPI Act, our business will observe caution when verifying clients' details using third-party data sources.
- 15.5. Our business acknowledges section 37(1) of the FIC Act which states that no duty of secrecy or confidentiality or any other restriction on the disclosure of information, whether imposed by legislation or arising from the common law or agreement, affects compliance by our business to report with the exception of the common law right afforded to legal professional privilege as between an attorney and the attorney's client noted in section 37(2) of the FIC Act in respect of communications made in confidence.
- 15.6. In terms of section 41A of the FIC Act, the FIC will ensure that it has appropriate measures in place to protect the confidentiality of personal information received by establishing and maintaining appropriate safeguards against the foreseeable internal and external risks identified.
- 15.7. In compliance with sections 21, 21A, 21B, 21C and 21E of the FIC Act, our business's FICA QUESTIONNAIRE includes questions in relation to our data subjects' personal information, our data subjects' occupation, our data subjects' general wealth profile, whether our data subjects may or may not be politically connected or not, whether our data subjects may receive benefit from any industry identified by the UN as higher risk (such as transportation businesses, courier businesses etc); and whether our data subjects hold business interests and/or bank accounts abroad.
- 15.8. We value our relationship with our clients and will keep all information supplied to us confidential in terms of our Data Privacy Terms and Conditions. Although we are very aware of the inconvenience of having to send and



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

resend the information and documents to the many institutions involved in the transaction, our business is bound by law in this regard and wish to avoid the possibility of all clients in the transaction, including ourselves, contravening the provisions in the FIC Act and the need in such instance, to address a report to the FIC.

16. AVAILABILITY AND REVISION

A copy of this Policy is made available on our business's website: www.aps-africa.com

This policy will continually be updated to comply with legislation, ensuring that personal information is secure.

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2024**

ANNEXURE A – BASIC CYBER SECURITY MEASURES IN PLACE



1. SOFTWARE AND CLOUD BASED SUPPORT PROGRAMS:

- 1.1. **Client Management System: KARBON**
- 1.2. **Central server/email management system: MICROSOFT 365**

2. BACKUPS:

- 2.1. Currently, the only backups being created are for the APS OneDrive data that is synced to the "server" located in South Africa.
- 2.2. These backups are currently being created using EaseUS Enterprise.
 - 2.2.1. Karbon backups are not done as all Karbon data resides on Karbon's Cloud Platform.
 - 2.2.2. Emails reside on M365's Cloud Platform and no local backups are created;
 - 2.2.3. No User devices are being backed up as All APS Data should reside in OneDrive and not locally on a Laptop or Desktop.
 - 2.2.4. User device data located in the Desktop, Documents and Pictures folders are synced to Each user's private section of OneDrive.

3. CYBER SECURITY:

3.1. Anti-Virus:

- 3.1.1. Devices procured with Windows 10/11Pro are covered by Windows Defender for Business via their assigned M365 Premium licensing.
- 3.1.2. Devices procured with Windows 10/11 Home are not covered by Windows Defender for Business but by the standard Windows Defender.

3.2. Firewalls:

- 3.2.1. No Firewall appliances are deployed as each employee works remotely with their own, personally procured ISPs, which falls outside the scope of our support.
- 3.2.2. Karbon and M365, however, have Firewall security in place on their respective Cloud Platforms, which



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

- 3.2.3. they manage as part of the licensing agreement with each company.
- 3.2.3. No central office or network/internet connection that can run behind a firewall.
- 3.2.4. No VPNs exist as there is no central office with servers or networks to connect to via VPN.
- 3.2.5. No Central Office is required for such infrastructure as all business operations currently run in the Cloud.

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2024**

REGULATED FORM 1

[documents \(dsd.gov.za\)](http://documents.dsd.gov.za)

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

**FORM 1
OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF
SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.
4 OF 2013)**

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
[Regulation 2(1)]**

- Note:
1. Affidavits or other documentary evidence in support of the objection must be attached.
 2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number....

A DETAILS OF DATA SUBJECT	
Name and surname of data subject:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
B DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party/(if the responsible party is a natural):	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
Name of public or private body/(if the responsible party is not a natural person):	
Business address:	

	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
C REASONS FOR OBJECTION (Please provide detailed reasons for the objection)	

Signed at this day of20

Signature of data subject (applicant)



APS Africa Consult (Pty) Ltd
 REGISTRATION NUMBER 2016/495511/07
 Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

REGULATED FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 3]

Note:

1. Affidavits or other documentary evidence as applicable in support of the request may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017 [Regulation 3(2)]

Note:

1. Affidavits or other documentary evidence in support of the request must be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

Reference Number....

Mark the appropriate box with an "x".

Request for:

- Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.
- Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A DETAILS OF THE DATA SUBJECT	
Surname:	
Full names:	
Identity number:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	
E-mail address:	
B DETAILS OF RESPONSIBLE PARTY	
Name and surname of responsible party (if the responsible party is a natural person):	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number:	

E-mail address:	
Name of public or private body (if the responsible party is not a natural person):	
Business address:	
Contact number(s):	Code ()
Fax number:	
E-mail address:	
C REASONS FOR "CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT"/"DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY. (Please provide detailed reasons for the request)	

* Delete whichever is not applicable

Signed at this day of 20.....

Signature of Data subject



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
DATA PRIVACY TERMS AND CONDITIONS
2024**



APS Africa Consult (Pty) Ltd
 REGISTRATION NUMBER 2016/495511/07
 Tel: 012 8832069 / www.aps-africa.com

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
 DATA PRIVACY TERMS AND CONDITIONS
 2024**

REGULATED FORM 3

APPLICATION FOR THE CONSENT OF A DATA SUBJECT FOR THE PROCESSING OF PERSONAL INFORMATION FOR THE PURPOSE OF DIRECT MARKETING IN TERMS OF SECTION 69(2) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013) REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 6]

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname/ registered name of data subject	
Unique identifier/identity number	
Residential, postal, or business address:	
	Code
Contact number(s):	
Fax number/E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/ registered name of responsible party or designated person	
Responsible party signature	
Unique identifier/identity number	
Residential, postal, or business address:	
	Code
Contact number(s):	
Fax number/E-mail address:	
C	GOODS OR SERVICES (Specify goods or services being marketed)
D	MARKETING METHOD (Specify marketing method, i.e., email)

My signature below confirms that I have consented to received direct marketing pertaining to the goods or services specified above by the means of the marketing method specified.

Signed at _____ this _____ day of _____ 20_____

 Signature of data subject/designated person



APS Africa Consult (Pty) Ltd
 REGISTRATION NUMBER 2016/495511/07
 Tel: 012 8832069 / www.aps-africa.com

**PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013
 DATA PRIVACY TERMS AND CONDITIONS
 2024**

DEFINITIONS

1. **“Biometric”**: means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
2. **“Child”**: means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;
3. **“Competent person”**: means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
4. **“Data subject”**: means the person to whom personal information relates and for the purposes of our business, this will include but not be limited to – tax and accounting services for both public and private entities and other general clients, employees, external service suppliers and all associates of our business;
5. **“Direct marketing”**: means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –
 1. Promoting or offering to supply, in the ordinary course of our business, tax and accounting services to the data subject; or
 2. Requesting the data subject to make a donation of any kind for any reason.
6. **“Electronic communication”**: means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
7. **“Filing system”**: means any structured set of personal information which in the case of our business consists of physical files kept in the offices of our business together with the data filed on the various software systems used by our business;
8. **“Information officer”**: of our business will mean **JOHAN RIEKERT**;
9. **“Our business”**: means –

BUSINESS NAME	APS AFRICA CONSULT (PTY) LTD
BUSINESS REGISTRATION NUMBER	2016/495511/07
BUSINESS ADDRESS: FIDUCIARY SERVICES	374 ANDERSON STREET, MENLO PARK, PRETORIA, 0081
BUSINESS ADDRESS: TAX AND ACCOUNTING	374 ANDERSON STREET, MENLO PARK, PRETORIA, 0081



APS Africa Consult (Pty) Ltd
REGISTRATION NUMBER 2016/495511/07
Tel: 012 8832069 / www.aps-africa.com

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

BUSINESS ADDRESS: TAX ON DECEASED ESTATES	705 WILLIAM NICOL DRIVE, ERASMUSKLOOF, PRETORIA, 0001
--	---

10. **“Person”**: means a natural person or a juristic person;
11. **“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:
 1. Information relating to the education or the medical, financial, criminal or employment history of the person;
 2. Any identifying number, symbol, e-mail address, telephone number, location information, online identifier or other particular assignment to the person;
 3. The biometric information of the person;
 4. The personal opinions, views or preferences of the person;
 5. Correspondence sent by the person that would reveal the contents of the original correspondence if the message is of a personal or confidential nature;
 6. The views or opinions of another individual about the person; and
 7. 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;
12. **“Private body”** means—
 1. A natural person who carries or has carried on any trade, business or profession, but only in such capacity;
 2. A partnership which carries or has carried on any trade, business or profession; or
 3. Any former or existing juristic person, but excludes a public body
13. **“Processing”**: means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –
 1. The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 2. Dissemination by means of transmission, distribution or making available in any other form; or
 3. Merging, linking, as well as restriction, degradation, erasure or destruction of information;
14. **“Promotion of Access to Information Act”**: means the Promotion of Access to Information Act (PAIA), 2000 (Act No. 2 of 2000);
15. **“Public record”**: means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.
16. **“Record”**: means any recorded information regardless of form or medium, including any of the following:
 1. Writing on any material;

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 DATA PRIVACY TERMS AND CONDITIONS 2024

-
2. Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
 3. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
 4. Book, map, plan, graph, or drawing;
 6. Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;
 7. In the possession or under the control of a responsible party; and
 8. Regardless of when it came into existence;
17. **“Regulator”**: – means the Information Regulator established in terms of Section 39 of the POPIA;
 18. **“Restriction”**: means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;
 19. **“Special personal information”**: means personal information as referred to in Section 26 of the POPIA which includes 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;
 20. **“This Act”**: means the Protection of Personal Information Act, No. 4 of 2013.
 21. **“Unique identifier”**: means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.