POPI COMPLIANCE POLICY

This policy sets out the relevant legislation and describes the steps taken to ensure compliance both in the processing of information, and as part of the introduction of new methods of processing, such as new IT systems.

APPLICATION

This policy covers all individuals working at all levels and grades, including managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual staff and volunteers (collectively referred to as staff or employees)

DEFINITIONS

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;

CLIENT
means the juristic and natural persons in respect of which services are provided, in terms of the Contract

CONTRACT
means the contract entered into between this organisation and its clients or staff or suppliers for the provision of services

DE-IDENTIFY
in relation to personal information of a data subject, means to delete any information that-

(a) identifies the data subject;
(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

GDPR
means the European Union General Data Protection Regulation

POPI
means the Protection of Personal Information Act 4 of 2013

PAIA
means the Promotion of Access to Information Act No. 2 of 2000

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-

(a) 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;
(b) information relating to the education or the medical, financial, criminal or employment history of the person;
(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
(d) the biometric information of the person;
(e) the personal opinions, views or preferences of the person;
(f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
(g) the views or opinions of another individual about the person; and
(h) 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;

It therefore means any information that relates to an identifiable person

PROCESS
means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
(b) dissemination by means of transmission, distribution or making available in any other form; or
(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

POLICY

In our business operations we make use of a variety of data about identifiable individuals (data subjects), including data about:

- Current, past and prospective employees
- Customers and clients
- Suppliers and vendors

In collecting and using this data, we are subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it. This includes compliance with POPI and PAIA.

It is our policy to ensure that compliance with the requirements of relevant legislation is clear and demonstrable at all times.

Where we process any information in respect of European Union citizens, we will ensure compliance with the requirements of GDPR, as this applies to any organisation processing data about European Union citizens, not just to organisations based within the European Union.

DATA PROTECTION OFFICER

In terms of GDPR, our business does not require a Data Protection Officer to be appointed. The CEO is the information officer in terms of POPI.

DATA PROTECTION PRINCIPLES

We are committed to processing data in accordance with our responsibilities and with data protection principles. This means ensuring that personal data is:

- processed lawfully, fairly and in a transparent manner

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes)

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

HOW WE COLLECT DATA

Our business may collect and receive personal data in a variety of ways. This includes the following:

- Physical documentation which is completed
- Data loaded onto our systems
- Data received from third parties, such as product suppliers, intermediaries, switches (Astute), employment agencies
- Telephone calls are voice logged
- Biometric entry systems etc.

Personal information will always be collected directly from the data subject, unless there is a good and lawful reason to collect information from a third party. If personal data is not obtained directly from the data subject, then the necessary disclosures will be provided to the data subject within a reasonable period after the data is obtained, but no longer than within one month.

We will ensure that we identify all areas where data is collected and ensure that the necessary privacy disclosures are made as required.

WHY WE COLLECT DATA

Personal information will only be collected for lawful reasons.

Our organisation uses personal information in furtherance of our legitimate interests in operating our services, website and business, and as required by applicable law. We also collect personal information to be able to comply with contractual obligations and to promote the interests of data subjects. More specifically, we collect information:

- To provide, update, maintain and protect our services, website and business. This includes use of personal information to support delivery of services under a client agreement, prevent or address service errors, security or technical issues, analyse and monitor usage, trends and other activities or at an Authorized User or Client's request.
- To communicate by responding to enquiries, requests, comments and questions. If we are contacted, we may use personal information to respond.
- To develop and provide search, learning and productivity tools and additional features. For example, we may improve search functionality by using information to help determine and rank the relevance of content, channels or expertise, make services suggestions based on historical use and predictive models, identify organizational trends and insights, to customize a services experience or create new productivity features and products.
- To send emails and other communications. We may send service, technical and other administrative emails, messages and other types of communications. We may also contact our clients and service providers to provide information about changes in our services, our services offerings, and important services-related notices, such as security and fraud notices. These communications are considered part of the services and you may not opt out of them.
- To provide services and comply with contractual obligations
- For billing, account management and other administrative matters. We may need to contact customers for invoicing, account management and similar reasons and we use account data to administer accounts and keep track of billing and payments.
- To analyse our performance
- To maintain a record of our contact and keep track of our interaction. This helps us provide a better level of service
- To quality assess the services provided and identify any areas for improvement and develop staff training
- To identify and analyse issues, risks and emerging trends in relation to the services we provide
- To process any complaints made against us
- To investigate and help prevent security issues and abuse.
- As required by applicable law, legal process or regulation.

Where information is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, we may use it for legitimate business purposes.

THE INFORMATION WE COLLECT

We shall ensure that personal data processed is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Where we enter into a business relationship with a party, data is required and personal information may be collected. The majority of the information is about the business, such as how it is structured and how it operates, but some personal data about employees, management, directors or shareholders may also occasionally be required (such as names, contact details) Where the party is a sole trader, much of the related information will also be personal data.

Where any financial products or services are provided, data which is collected is required in order for us, and our product providers, to provide the required services. This includes both personal data and special personal data and may include children's information.

Depending on the reason we are contacted, we may also collect other personal data about the individual which the person has chosen to provide. We may receive additional information should a person participate in a focus group, contest, activity or event, apply for a job, request support, submit a complaint, interact with our social media accounts or otherwise communicate with us.

Sensitive personal information such as bank account information is collected in order to process salaries and wages of internal staff, staff benefits, taxation, payments and receipts from suppliers, vendors and clients, and for onward transmission to suppliers where we act as intermediary for the supply of services.

Some special categories of personal data may be included in the information that we collect or record. To the extent that we do process any special categories of data as part of our work, this will be done in compliance with legislative requirements.

CONTRACTS INVOLVING THE PROCESSING OF PERSONAL DATA

[NAME OF ORGANISATION] will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract, where applicable, that includes the specific information and terms required by regulation. ("Agreement")

DATA ACCURACY

Reasonable steps shall be taken to ensure data is accurate at all times. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

If personal information held is inaccurate or incomplete, the data subject can request that it be updated. This request must be submitted on the appropriate form and according to internal procedure which may be accessed from our offices.

PROCESSING PERSONAL DATA

It is our policy to identify the appropriate basis for processing personal data and to document this. All data processed shall be done on one or more of the following lawful bases:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests of the organisation

CONSENT

Unless legally permitted, we will always obtain consent from a data subject to collect and process their data.

Transparent information about our usage of personal data will be provided to data subjects at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

Where consent is relied upon as a lawful basis for processing data, evidence of this shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent shall be clearly available and systems shall be in place to ensure such revocation is reflected accurately.

PERFORMANCE OF A CONTRACT

Where personal data collection and processing is required to fulfil a contract with the data subject, explicit consent from the data subject is not required. This applies where the contract cannot be completed without the personal data in question.

LEGAL OBLIGATION

If personal data is required to be collected and processed in order to comply with a prevailing law, then explicit consent is not required. This may be the case for some data related to employment and taxation for example.

VITAL INTERESTS OF A DATA SUBJECT

Where personal data is required to protect the vital interests of a data subject or of another natural person, then this may be used as the lawful basis of the processing. We will retain reasonable, documented evidence that this is the case where this reason is used as the lawful basis of processing.

TASK CARRIED OUT IN THE PUBLIC INTEREST

Where the business needs to perform a task that it believes is in the public interest then the data subject's consent will not be requested. The assessment of the public interest will be documented and made available as evidence where required.

LEGITIMATE INTERESTS

If the processing of specific personal data is in the legitimate interests of the organisation and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. The reasoning behind this view will be documented in such instance.

FURTHER PROCESSING OF PERSONAL INFORMATION

We will only process personal information for the purpose for which it was collected. Any further processing, including the keeping of records, will only be permitted where this is lawful and justified.

DATA RETENTION

Our business retains data in accordance with instruction, any applicable terms in agreements, use of services functionality, and as required by applicable law. This may include keeping information after accounts have been deactivated for the period of time needed for us to pursue legitimate business interests, conduct audits, comply with (and demonstrate compliance with) legal obligations, resolve disputes and enforce our agreements.

To ensure that personal data is kept for no longer than necessary, we shall consider what data should or must be retained, for how long, and why, and ensure procedures are implemented to give effect to this.

Where required, we will obtain the required consents to retain personal information for longer periods.

DATA SECURITY

We take the security of personal data very seriously and take all reasonable measures to protect data from loss, misuse, and unauthorized access or disclosure.

We will implement a risk-based information security program, taking into consideration Generally Accepted Security Practices.
These steps take into account the sensitivity of information we collect, process and store, and the current state of technology. Access to personal data shall be limited to persons who need access and appropriate security shall be in place to avoid unauthorised sharing of information.

Electronically held personal data shall be stored securely using appropriate software that is kept-up-to-date. Appropriate back-up and disaster recovery solutions shall be in place.

Measures will be implemented to ensure that personal information is only processed for the purpose for which it was collected, and for no other purpose, unless lawfully permitted.

CONTINUAL IMPROVEMENT OF INFORMATION SECURITY

Our policy with regard to continual improvement is to:

- Continually improve the effectiveness of information security controls
- Enhance current processes to bring them into line with good practice as defined within relevant standards
- Increase the level of pro-activity with regard to information security
- Review ideas for improvement at regular management meetings in order to prioritise and assess timescales and benefits

Ideas for improvements may be obtained from any source including employees, clients, suppliers, IT staff, risk assessments and service reports. Once identified, these will be recorded and evaluated as part of management reviews.

PRIVACY BY DESIGN

Our business will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data
- What controls are necessary to address the identified risks and demonstrate compliance with legislation

TRANSFERRING PERSONAL DATA

Although unlikely, we may transfer personal data to countries other than South Africa. Before we transfer personal data, we have procedures to ensure that appropriate safeguards are put in place to protect any personal data included in such a transfer
We deploy the following safeguards if we transfer personal data

Where we transfer personal information outside South African borders, we will satisfy ourselves as to the levels of security of the destination, and only transfer data where this is at least equal to the data protection requirements locally. Where this is not the case, we will ensure that we obtain the necessary consent, and will provide full disclosure to the data subjects.

DATA DELETION

Data subjects may request us to stop holding or using their information, which we will do unless we have genuine and lawful reasons for continuing to hold or use it. Data which may no longer lawfully be retained will be permanently and completely deleted.

The deletion of Customer Data and other use of the services by clients and customers may result in the deletion and/or de-identification of certain associated Information.

CONFIDENTIALITY AND ACCESS RIGHTS

We respect the right of access. Where we are requested to confirm whether we have any personal information, we will ensure that the following information is provided to the person making the request, where lawful and applicable:

- whether we hold any such information:
- a description of it
- reasons why we are holding it
- details of any person to whom it could be or has been disclosed
- details of how long we intend to keep the information
- details of where we obtained the information (if not from the enquirer directly)
- full details, if any significant automated decisions (those made by a computer and with no human intervention) have been made about by us
- a copy of the information in an intelligible form

Subject access requests require us to provide a copy of any personal data pertaining to the person submitting this request. Internal procedures will ensure compliance with PAIA data subject access rights.

SHARING AND DISCLOSING INFORMATION

We will share and disclose data solely in accordance with the data subject's instructions, including any applicable terms in any applicable agreement and use of services functionality, and in compliance with applicable law and legal process.

Except as expressly permitted or in cases of emergency to avoid death or physical harm to individuals, we will only disclose data in response to valid and binding compulsory legal process. Any person issuing legal process or legal information requests (e.g., discovery requests, warrants, or subpoenas) is required to do so in accordance with prevailing regulation and jurisdiction.

Where we are required to disclose or share data due to legal process, we will notify the data subject before disclosing any data, so that such person may seek protection from such disclosure, unless we are prohibited from doing so or there is a clear indication of illegal conduct or risk of harm to people or property associated with the use of such data.

Where we are legally prohibited from notifying the data subject prior to disclosure, we will take reasonable steps to notify the person of the demand after the non-disclosure requirement expires.

DATA BREACH

Clear procedures shall be implemented to ensure that we can detect quickly any data breach, react appropriately and notify in time where required. These shall be included in our Information Security Incident Response Procedure

It is our policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, we shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the appropriate Regulators. If required, individuals affected will be notified.

Where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours.

TRAINING

We will ensure that all staff are appropriately trained, and receive ongoing training, in order to ensure compliance with this policy.

ENFORCEMENT

Any staff member who contravenes this policy will be subject to disciplinary sanction, up to and including dismissal.

If you have any questions or would like to understand more about POPIA, Please contact us through any of the following ways.

Contact Centre: 012 054 6158
Client and Adviser Service Centre: alistair@metrofin.co.za
Group Information Officer – Adolf Fick: - Email adolf@metrofin.co.za