three6five
empowering digital communications

+27 86 0000 365
+27 11 4634 665.
+27 86 6440 228

13 Challenger Avenue
International Business
New Road
Midrand, 685

PO Box 535
Fourways North
Johannesburg
2086

info@three6five.com

three6five.com

32. POPIA POLICY

32.1 Introduction:

The right to privacy is an integral human right recognised and protected in the South African Constitution in the Protection of Personal Information Act 4 of 2012 ("POPIA")

POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.
Through the provision of quality goods and services three6five, is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of client, customers and team members.

A person's right to privacy entails having control over his/her personal information and having the ability to conduct his/her affairs relatively free from unwanted intrusions.

Given the importance of privacy three6five is committed to effectively managing personal information in accordance with POPIA's provisions.

32.2 Mission:

The mission of this policy is to be sensitive to the personal nature of the information customers, client and/or team members provide to three6five. This policy explains how three6five will protect and use Personal Information.
three6five will not use Personal Information for any other purpose than that set out in this Policy and our Privacy Policies (loaded on our website) and will endeavour to protect your Personal Information that is in our possession from unauthorised alteration, loss, disclosure and/or access.
This Policy extends to external parties with whom three6five interact, including but not limited to individual clients, representatives of client organisations, visitors to three6five offices, and other users of our services.
Where three6five needs to process your Sensitive Personal Information, it will done so in the ordinary course of business, for a legitimate purpose, and in accordance with the applicable law.

32.3 Definitions:

32.3.1 *Personal Information*: Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural persona, and where applicable, and identifiable, existing juristic person (such as a company) including but not limited to the information concerning:

- Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical and/or mental health, disability, religion, conscience, belief, culture language and birth of a person;
- Information relating to the education or the medical, financial, criminal or employment history of the person;
- Any identifying number, symbol, email address, physical address, telephone number, locations information, online identifier or other particular assignment to the person;
- The biometric information of the person;
- Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- The views or opinions of another individual about the person;
- 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 reveals information about the person.

32.3.2 Date Subject: This refers to the natural or juristic person to whom the personal information relates, such as an individual
client, customer or a company that supplies three6five with products or other goods.

32.3.3 Responsible Party: The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of the means for processing the personal information. In this case three6five is the responsible party.

32.3.4 Operator: An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third party service provider that has contracted three6five to shred documents containing personal information. When dealing with and operator, it is considered good practice for a responsible party to include an indemnity clause.

32.3.5 Information Officer: The Information Officer/s is responsible for ensuring three6five's compliance with POPIA. Where no information offices is appointed, the CEO of three6five will be responsible for performing the Information Officer duties.
Once appointed, the Information Officer must be resisted with the South African information Regulator established under POPIA prior to performing his/her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

32.3.6 Processing: The act of processing information includes any activity or any set of operations, whether or not automatic means, concerning personal information and includes:

- The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- Dissemination by means of transmission, distributing or making available in any other form; or
- Merging, linking as well as any restriction, degradation, erasure or destruction of information.

32.3.7 Record: Means any recorded information, regardless of form or medium, including:

- Writing on any material;
- 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;
- Label, making or other writing that identifies or describes anything of which it forms part or to which it is attached by any means;
- Book, map, plan, graph or drawing;
- Photograph, film, negative, tape or other device in which one or more visual images are embodied so as the be capable, with or without the aid of some other equipment, of being reproduced.

32.3.8 Filing System: Means any structed set of personal information, whether centralised, de3centralised or dispersed on a functional or geographical basis, which is accessible according to the specific criteria.

32.3.9 Unique Identifier: Means any identifier that is assigned to a date subject and is used by a responsible party for the purpose of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

32.3.10 De-Identify: This means to delete any information that identifies a data subject or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

32.3.11 Re-Identify: In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

32.3.12 Consent: Means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

32.3.13 Direct Marketing: Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

- Promoting or offering to supply, in the ordinary course of business, any goods or services to the date subject; **or**
- Requesting the date subject to make a donation of any kind for any reason.

32.3.14 Biometrics: 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.

32.4 Purpose*:*

This purpose of this policy is to protect **t**hree6five from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, **t**hree6five could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose **t**hree6five uses information relating to them.
- Reputational damage. For instance, **t**hree6five could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by **t**hree6five.

This policy demonstrates **t**hree6five is commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of **t**hree6five.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of **t**hree6five and data subjects.
- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

32.5 Organisational Scope:

This policy and its guiding principles applies to:

- **t**hree6five POPIA Committee
- All branches, business units and divisions of **t**hree6five
- All team members and volunteers
- All contractors, suppliers and other persons acting on behalf of MHA

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- A processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded in the course of purely personal or household activities, or
- where the personal information has been de-identified.

32.6 Rights of Data Subjects:
Where appropriate, **t**hree6five will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. **t**hree6five will ensure that it gives effect to the following seven rights:

32.6.1 The right to access Personal Information:
three6five recognises that a data subject has the right to establish whether **t**hree6five holds personal information related to him, her or it including the right to request access to that personal information. An example of a "Personal Information Request Form" can be found under Annexure A.

32.6.2 The right to have Personal Information corrected or deleted:
The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where **t**hree6five is no longer authorised to retain the personal information.

32.6.3 The right to object to the processing of Personal Information:
The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.
In such circumstances, **t**hree6five will give due consideration to the request and the requirements of POPIA. **t**hree6five may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

32.6.4 The right to object to Direct Marketing:
The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

32.6.5 The right to complain to the Information Regulator:
The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information. An example of a "POPI Complaint Form" can be found under Annexure B.

32.6.6 The right to be informed:
The data subject has the right to be notified that his, her or its personal information is being collected by . **t**hree6five. The data subject also has the right to be notified in any situation where . **t**hree6five has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

32.7 Specific Duties and Responsibilities:
32.7.1 POPIA Committee:
three6five's POPIA Committee cannot delegate its accountability and is ultimately answerable for ensuring that the organisation meets its legal obligations in terms of POPIA. The committee may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The POPIA Committee is responsible for ensuring that:

- **t**hree6five appoints an Information Officer/s, and where necessary, a Deputy Information Officer/s.

- All persons responsible for the processing of personal information on behalf of the organisation:
    - are appropriately trained and supervised to do so;
    - understand that they are contractually obligated to protect the personal information they come into contact with, and
    - are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.
- Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so.
- The scheduling of a periodic POPIA Audit in order to accurately assess and review the ways in which three6five collects, holds, uses, shares, discloses, destroys and processes personal information.

32.7.2 Information Officer:

three6five Information Officer/s is responsible for:

- Taking steps to ensure three6five's reasonable compliance with the provision of POPIA.
- Keeping the POPIA Committee updated about three6five's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the committee of their obligations pursuant to POPIA.
- Continually analysing privacy regulations and aligning them with three6five's personal information processing procedures. This will include reviewing three6five's information protection procedures and related policies.
- Ensuring that POPIA Audits are scheduled and conducted on a regular basis.
- Ensuring that three6five makes it convenient for data subjects who want to update their personal information or submit POPIA related complaints to three6five. For instance, maintaining a "contact us" facility on three6five intranet.
- Approving any contracts entered into with operators, team members and other third parties which may have an impact on the personal information held by three6five. This will include overseeing the amendment of three6five's employment contracts and other service level agreements.
- Encouraging compliance with the conditions required for the lawful processing of personal information.
- Ensuring that team members and other persons acting on behalf of three6five are fully aware of the risks associated with the processing of personal information and that they remain informed about three6five security controls.
- Organising and overseeing the awareness training of team members and other individuals involved in the processing of personal information on behalf of three6five.
- Addressing team members' POPIA related questions.
- Addressing all POPIA related requests and complaints made by three6five data subjects.
- Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, with regard to any other matter.

The Deputy Information Officer will assist the Information Officer in performing his or her duties.

32.7.3 Chief Technical Officer:

three6five's Chief Technical Officer is responsible for:

- Ensuring that three6five IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
- Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
- Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
- Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
- Ensuring that all back-ups containing personal information are protected from

unauthorised access, accidental deletion and malicious hacking attempts.
- Ensuring that personal information being transferred electronically is encrypted.
- Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
- Performing regular IT audits to ensure that the security of **t**hree6five's hardware and software systems are functioning properly.
- Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
- Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on **t**hree6five's behalf. For instance, cloud computing services.
- Approving and maintaining the protection of personal information statements and disclaimers that are displayed on **t**hree6five website, including those attached to communications such as emails, intranet and electronic newsletters.
- Addressing any personal information protection queries from journalists or media outlets such as newspapers.
- Where necessary, working with persons acting on behalf of **t**hree6five to ensure that any outsourced marketing initiatives comply with POPIA.

32.7.4 Team Members and other persons acting of behalf of **t**hree6five *:*
Team Members and other persons acting on behalf of **t**hree6five will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other team members.
Team Members and other persons acting on behalf of **t**hree6five are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
Team Members and other persons acting on behalf of **t**hree6five may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within **t**hree6five or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the team members or person to perform his, her or its duties.
Team Members and other persons acting on behalf of **t**hree6five must request assistance from their Team Leader/Manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of three6five will only process personal information where:
- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of **t**hree6five or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:
- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted **t**hree6five with explicit written or verbally recorded consent to process his, her or its personal information.

Team Members and other persons acting on behalf of **t**hree6five will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, **t**hree6five will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Team Members and other persons acting on behalf of **three6five** will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from **three6five's** central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant Team Leader/Manager, the Information Officer/s or Human Resources.
- Transfer personal information outside of South Africa without the express permission from the Information Officer.

Team Members and other persons acting on behalf of **three6five's** are responsible for:

- Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
- Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
- Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist team members where required, other persons acting on behalf of **three6five**, with the sending or sharing of personal information to or with authorised external persons.
- Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
- Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.
- Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
- Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant Team Leader/Manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant Team Leader/Manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPIA Awareness training from time to time.

Where a team member, or a person acting on behalf of **three6five**, becomes aware or

suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

32.8 POPIA Audit:

three6five Information Officer will schedule periodic POPIA Audits. The purpose of a POPIA audit is to:

- Identify the processes used to collect, record, store, disseminate and destroy personal information.
- Determine the flow of personal information throughout **t**hree6five. For instance, **t**hree6five's various business units, divisions, branches and other associated organisations.
- Redefine the purpose for gathering and processing personal information.
- Ensure that the processing parameters are still adequately limited.
- Ensure that new data subjects are made aware of the processing of their personal information.
- Re-establish the rationale for any further processing where information is received via a third party.
- Verify the quality and security of personal information.
- Monitor the extend of compliance with POPIA and this policy.
- Monitor the effectiveness of internal controls established to manage three6five POPIA related compliance risk.

In performing the POPIA Audit, Information Officers will liaise with Team Leaders/Managers in order to identify areas within in **t**hree6five's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from Team Leaders/Managers and **t**hree6five's POPIA Committee in performing their duties.

32.9 Request to access Personal Information:

Data subjects have the right to:

- Request what personal information **t**hree6five holds about them and why.
- Request access to their personal information.
- Be informed how to keep their personal information up to date.

Access to information requests can be made via email, addressed to the Information Officer. The Information Officer will provide the data subject with a "Personal Information Request Form". Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against **t**hree6five PAIA Policy. The Information Officer will process all requests within a reasonable time.

32.10 POPIA Complaints Procedure:

Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. **t**hree6five takes all complaints very seriously and will address all POPIA related complaints in accordance with the following procedure:

- POPIA complaints must be submitted to **t**hree6five in writing. Where so required, the Information Officer will provide the data subject with a "POPIA Complaint Form"
- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.
- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
- The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavour to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.
- The Information Officer must also determine whether the complaint relates to an error or

breach of confidentiality that has occurred and which may have a wider impact on **t**hree6five's data subjects.

- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with **t**hree6five's POPIA Committee where after the affected data subjects and the Information Regulator will be informed of this breach.
- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to **t**hree6five's POPIA Committee within 7 working days of receipt of the complaint. In all instances, **t**hree6five will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
- The Information Officer's response to the data subject may comprise any of the following:
    - A suggested remedy for the complaint,
    - A dismissal of the complaint and the reasons as to why it was dismissed,
    - An apology (if applicable) and any disciplinary action that has been taken against any team members involved.
    - Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.
    - The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPIA related complaints.

32.11 Disciplinary Action:

Where a POPIA complaint or a POPIA infringement investigation has been finalised, **t**hree6five may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any team member reasonably suspected of being implicated in any non-compliant activity outlined within this policy.

In the case of ignorance or minor negligence, **t**hree6five will undertake to provide further awareness training to the team member.

Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which **t**hree6five may lead to the dismissal of the team member. Disciplinary procedures will commence where there is sufficient evidence to support a team members gross negligence.

Examples of immediate actions that may be taken subsequent to an investigation include:

- A recommendation to commence with disciplinary action.
- A referral to appropriate law enforcement agencies for criminal investigation.
- Recovery of funds and assets in order to limit any prejudice or damages caused.