☎ +27 86 000 6335
🖷 +27 86 206 6975
✉ service@odek.co.za
www.odek.co.za
Block A1, 8 Hillside Road, Parktown, 2193

COMPLIANCE POLICY IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA)

("The Policy")

FOR

ODEK Alliance

ODEK Technologies (Pty) Ltd with registration number: 2013/200267/07;

ODEK AppCraft (Pty) Ltd with registration number: 2016/056260/07;

ODEK Accendo (Pty) Ltd with registration number: 2019/477466/07;

ODEK Telecoms (Pty) Ltd with registration number: 2018/074446/07;

ODEK AppCraft India with company identity number: U72200PN2018PTC177771;

ODEK Emporium (Pty) Ltd with registration number: 2018/364965/07;

ODEK Money (Pty) Ltd with registration number: 2018/567395/07;

ODEK Capital (Pty) Ltd with registration number: 2018045710/07;

ZARODEK (Pty) Ltd with registration number: 2017/374060/07;

TIODEK Administration (Pty) Ltd with registration number: 2018/045741/07

TIODEK (RF) with registration number: 2018/405929/07

TIODEK Business Structures (Pty) Ltd with registration number: 2018/045749/07

("ODEK")

Table of Contents

1. THE AIM OF THE POPIA COMPLIANCE POLICY

1.1. Background

ODEK as a responsible party and in some instances, an operator has the responsibility to ensure that data is kept safe. ODEK has always been committed to protecting the clients and/or users' privacy by processing Personal Information and Special Personal Information lawfully, properly and transparently. The Policy sets out what personal information ODEK processes, why it is processed and who it is sent to and/or received from. In addition, POPIA is placing an additional burden of care relating to data security on all entities to be adhered to.

1.2. The aim of the POPIA Compliance Policy

The Policy aims to ensure that ODEK protects the clients' and/or users' Personal Information and Special Personal Information, whilst adhering to all relevant legislation including but not limited to FICA (Financial Intelligence Centre Act No 38 of 2001), PAIA (Promotion of Access to Information Act No 2 of 2000) and POPIA.

1.3. The principles of the POPIA Compliance Policy

- Data collection;
- Data processing;
- Data storage;
- Data privacy;
- Destruction of data (where and when applicable).

1.4. Important POPIA Definitions

- "Biometrics" means the measurement and statistical analysis of people's unique physical and behavioural characteristics. The technology is mainly used for identification and access control;

- "Consent", means the voluntary, specific and informed expression of will in terms of which permission is given for the processing of Personal Information and Special Personal Information. If clients and/or users have read the ODEK privacy policy, accepted the terms and conditions and provided ODEK with the required Personal Information and/or Special Personal Information, the client and/or user has consented to the use of the data. If the client and/or user wishes for ODEK to stop making use of the data, they must expressly inform ODEK of such request. Clients and/or users must be informed that if ODEK is unable to process the data, ODEK may be unable to provide certain services to the client and/or user;
- "Data Subject", herein referred to as the "client and/or user" and means a natural person or a juristic person to whom the personal information relates;
- "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;
- "Operator" means a person or entity who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. Where a party processes personal information as an operator, it must secure the integrity and confidentiality of that personal information by taking appropriate, reasonable technical and organisation measures to prevent loss of, damage to or unauthorised destruction of the personal information and unlawful access to or processing of the personal information. This may include but is not limited to, verification agencies, advertising and public relations agencies, call centres, service providers, auditors, legal practitioners, organs of state, government, provincial and municipal bodies;
- "Personal Information" means personal information relating to any identifiable, living, natural person, and an identifiable, existing juristic person, including, but not limited to the person's
    - race, sex, gender, sexual orientation, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being,

disability, religion, conscience, belief, cultural affiliation, language and birth;

- education, medical, financial, criminal or employment history;
- identifying number, pin code, customer or code or number, numeric, alpha, or alpha-numeric design or configuration of any nature, symbol, e-mail address, physical address, cellular phone number, telephone number or other particular assignment which can be decoded to reveal information on the person;
- blood type, fingerprint or any other biometric information;
- personal opinions, views or preferences;
- correspondence that is implicitly or explicitly of a personal, private or confidential nature (or further correspondence that would reveal the contents of the original correspondence);
- views or opinions of another individual about the person; and
- the person's name, if it appears with other personal information relating to such person or if the disclosure of the name itself would reveal information about the person;

- "Processing" / "process" or processed", means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including - the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; or merging, linking, as well as restriction, degradation, erasure or destruction of information. This includes all types of usage of a client and/or users personal information including the initial processing the data is collected and any further and ongoing processing. Processing must be done in a lawful, legitimate and responsible manner and in accordance with the provisions, principles and conditions set out under POPIA;

- "Responsible Party" means a public or private body or any person which, alone or in conjunction with others, determine the purpose of and means for processing personal information;
- "Special Personal Information" means personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to- the alleged commission by a data subject of any offence, or any proceedings in respect of any offence allegedly committed by the data subject or the disposal of such proceedings. Special Personal Information may only be processed subject to certain exceptions as set out in POPIA.

1.5. **Processing**

- POPIA encourages responsibility, security, and consent. Personal information may only be processed where-
    - Processing is necessary to carry out actions for the conclusion or performance of a contract to which the client and/or user of the personal information is a party;
    - Processing is required in order to comply with an obligation imposed by the law;
    - Processing is necessary to protect a legitimate interest of the data subject ;
    - Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied; or
    - Processing is necessary for the proper performance of a public law duty by a public body or on behalf of a public body.
- Processing special personal information is permitted only where –
    - Consent is obtained from the data subject;
    - It is necessary by law;

- Is done for historical, statistical or research purposes that is in the public interest;
- The information has been deliberately made public by the data subject.

- Processing personal information of a minor (under the age of 18 years) is prohibited unless one of the following justifications are met -
  - A parent or guardian may consent to the processing;
  - It is necessary for the establishment, exercise or defence of a right or obligation in law (which includes obligations of international public law);
  - It is done for historical, statistical or research purposes that is in the public interest;
  - If the child deliberately made the personal information public with the consent of a parent or guardian.

1.6. **The purpose of this document**

- To ensure compliance with all the relevant legislation;
- The aim is to focus on POPIA;
- This POPIA Policy applies to interactors, users of the ODEK sites and applications, clients, contractors, service providers, regulators and public bodies, employees, business partners and affiliates.

2. KEY CONCEPTS

2.1. Develop, implement, monitor and maintain a compliance framework;

2.2. Perform information assessments;

2.3. Create awareness;

2.4. Confidentiality and Non-Disclosure Agreements;

2.5. Ensure compliance;

2.6. Continuous management.

3. ROLES AND RESPONSIBILITIES

The persons appointed to take full responsibility for the policy.

3.1. **Information Officer for ODEK Technologies and ZarODEK:**

- Information Officer: Karien Greeff
- Date of appointment: 11 June 2021
- Email Address: karieng@odek.co.za

*** This person has the required authority to manage and attend to all information related matters***

This person takes full responsibility for the implementation of the POPIA Compliance Policy within ODEK Technologies and ZARODEK.

3.2. **Information Officer for ODEK Accendo, ODEK AppCraft, ODEK AppCraft India, ODEK Telecoms, ODEK Money, ODEK Capital, TIODEK and ODEK Emporium:**

- Information Officer: Leopold Johann Malan
- Date of appointment: 11 June 2021
- Email Address: leopoldm@odek.co.za

*** This person has the required authority to manage and attend to all information related matters***

This person takes full responsibility for the implementation of the POPIA Compliance Policy within ODEK Accendo, ODEK AppCraft, ODEK AppCraft India, ODEK Telecoms, ODEK Money, ODEK Capital, TIODEK and ODEK Emporium.

3.3. **Deputy Information Officer for ODEK Accendo:**

- Information Officer: Nadine dos Santos
- Date of appointment: 11 June 2021
- Email Address: nadineb@odek.co.za

ODEK will ensure that it performs regular audits regarding the safety and the security of all data subject's personal information.

3.4. **The role of all employees**

- All employees will have to comply with the policy, and everything related to POPIA together with the ODEK Alliance PAIA Manual;
- Employees will have to identify personal information in their day-to-day duties and ensure that all measures are adhered to;
- When obtaining personal information for a juristic person (company), the employee should ensure that the person representing the juristic person has the necessary authority to act on behalf of the juristic person and that they have the right to provide ODEK with the personal information and/or the required permission with regard to processing the information;
- Employees will notify their team managers and the Director of the Company of any breach of personal information immediately so that the necessary action may be taken;
- All employees have signed new Confidentiality and Non-Disclosure Agreements.

3.5. **The POPIA Policy and other Governance Risk and Compliance departments**

The POPIA policy is in line with the following internal policies of ODEK:

- *Information and Data Security;*
- *Compliance;*
- *Privacy;*
- *Risk Management.*

4. POLICY DEVELOPMENT, ALIGNMENT AND IMPLEMENTATION

4.1. Purpose

- ODEK collects and processes personal information pertaining to their clients and/or users' only for the purpose for which it was collected and in the ordinary course of business, for example:
    - Contract purposes and due diligence;
    - To process transactions and render services;
    - To administer accounts and profiles for billing, quoting and invoicing i.e. financial management;
    - To conduct risk assessments, anti-bribery and corruption assessments;
    - For legal obligations and public duties;
    - For security purposes;
    - To verify bank account or credit card details and, where authorised, use that information to process payments;
    - To confirm and verify identities, you consent to the collection, processing and storing of biometric data such as fingerprint recognition, facial recognition and/or ID photo verification;
    - To detect and prevent fraud and/or crime and recover debts;
    - To provide updated information on rates and amended terms and conditions;
    - To respond to requests for information regarding products, services, software and pricing information;
    - For marketing and/or to offer new or additional services and/or provide information on products, software and/or services, only if the client and/or user has consented to such marketing;

- To conduct client satisfaction surveys, only if the client and/or user has consented to such service.

4.2 Collection

- A client's and/or users' consent (voluntary, specific and informed) is required to collect and process personal information. An accepted written agreement or online acceptance of terms and conditions together with receipt of the relevant compliance documents constitutes consent. By using the online services, the products and services and/or communicating electronically and/or using non-electronic means of communication, the client and/or user agrees to this policy and consents to the collection, processing and transfer of their information as set out in this policy. ODEK processes personal information to provide access to products and/or services and/or software. Examples of personal information collected by ODEK includes, but is not limited to:

  Company:

  - Company name;
  - Registration number;
  - SARS documentation;
  - Registered address;
  - Contact details;
  - Bank details;
  - Subscriber details
  - Biometric Data (Fingerprints, ID Photo and/or Facial Recognition).

  Individual:

  - Name and surname;
  - Physical address;
  - Contact details;
  - ID and/or passport number;
  - Bank details;

- Subscriber details
- Biometric Data (Fingerprints, ID Photo and/or Facial Recognition).

- ODEK will further collect, device and browser Information, such as network and connection information (including Internet Service Provider (ISP) and Internet Protocol (IP) addresses), device and browser identifiers and information (including device, application, or browser type, version, plug-in type and version, operating system, user agent, language and time zone settings, and other technical information), advertising identifiers, cookie identifiers and information, and similar data, which are required to perform contractual matters and / or in order to provide the client and/or user access to services or attend to queries or to ensure that security safeguards are in place;

- Further, ODEK will collect information and browsing history, such as usage metrics (including usage rates, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs), content interactions (including searches, views, downloads, prints, shares, streams, and display or playback details), and user journey history (including clickstreams and page navigation, URLs, timestamps, content viewed or searched for, page response times, page interaction information (such as scrolling, clicks, and mouse-overs, and download errors), advertising interactions (including when and how the clients and/or users interact with marketing and advertising materials, click rates, purchases or next steps the clients and/or users may make after seeing an advertisement, and marketing preferences), and similar data which are required to perform contractual matters and / or in order to provide the client and/or user access to services or attend to queries or to ensure that security safeguards are in place.

- Records of consent given by the client and/or user in the form of written consent, online consent and voice recordings will be kept with the date and time, means of consent and any related information.

4.3 Sources of information

- ODEK will collect and obtain the personal information either directly from the data subject, automatically or from third parties as follows:

  Direct collection:

  - Create or maintain a profile or account with ODEK;
  - Conclude a contract with ODEK;
  - Purchase, subscribe or use of ODEK services;
  - Purchase, use, or otherwise interact with content, products, or services from third party providers who have a relationship with ODEK;
  - Request or sign up for information, including marketing material;
  - Communicate with ODEK by phone, email, chat, in person, or otherwise.

  Automatic collection:

  - Search for, visit, interact with, or use the ODEK website, applications, mobile applications, or social media portals or platforms;
  - Use ODEK goods or services (including through a device);
  - Access, use, or download content from ODEK;

  Collection from third parties:

  - Service providers and business partners who work with ODEK and that ODEK may utilise to deliver certain content, products, or services or to enhance client and/or user experience;

- SAPS, Home Affairs, Credit bureaus and other similar agencies;
- Government agencies, regulators and others who release or publish public records;
- Other publicly or generally available sources, such as social media sites, public and online websites, open databases, and data in the public domain.

4.4 Storing data:

- ODEK uses standard industry practices to safeguard the confidentiality of personal information. The data is treated as an asset that must be protected against loss and unauthorised access. ODEK employs many different security techniques to protect such data from unauthorised access. Electronic and hardcopy information (when required) is stored at the ODEK head office in Johannesburg, South Africa or at other secure site/s and information is encrypted wherever possible;
- ODEK keeps back-ups of personal information and data if the client and/or user consents to the collection and storage of such data.

4.5 It is advisable that a client and/or user is informed that the information collected will be kept for a period of 5 years after the relationship between ODEK and the client and/or user has been terminated in terms of FICA;

4.6 Data security is of the utmost importance. It is also vital to note that ODEK only retains data that is part of the transaction with the client and/or user;

4.7 The data breach policy will form an essential part of the POPIA Compliance Policy and this document will be updated as and when required;

4.8 Data security will be tested on a regular basis;

4.9 Breach handling and escalation will be part of the responsibilities of the POPIA Information Officer/s. A register of incidents will be kept with actions taken where applicable;

4.10 ODEK has always and will continue to ensure that there is access control to all areas where data is kept. This includes strong passwords, no use of USB's or external hard drives allowed and building access control.

5. SHARING INFORMATION

5.1. ODEK will under no circumstances sell or commercialise personal information or data unless consent is obtained. Whereafter the data will be sold or commercialised in the format agreed to between ODEK and the data subject.

5.2. The ODEK Alliance, ODEK employees and the ODEK affiliates will have access to a data subjects' personal information.

6. RISK ASSESSMENTS

6.1. POPIA will be added to the data breach policy and it will be updated regularly;

6.2. ODEK will assess risks and breach incidents to establish the magnitude.

7. ACCESS BY OTHERS AND CROSS BORDER TRANSFER

7.1. ODEK may from time to time disclose data to other parties, including holding companies or subsidiaries, third party service providers and processors, cyber service providers, trading partners, agents, auditors, organs of state, regulatory bodies and / or national governmental, provincial, or local government municipal officials, or overseas trading parties or agents, but such disclosure will always be subject to an agreement which will be concluded between ODEK and the party to whom the data is disclosed, which contractually obliges the recipient of the data to comply with strict confidentiality and data security conditions in line with POPIA;

7.2 Where data must be transferred to a country situated outside the borders of South Africa, the data will only be transferred to countries which have similar data privacy laws in place or where the recipient of the data concludes an agreement which contractually obliges the recipient to comply with strict confidentiality and data security conditions and which in particular will be to a no lesser set of standards than those imposed by POPIA;

7.3 In addition to the data stored in point 4.4 above, ODEK stores data outside the borders of South Africa (including but not limited to) in Sharepoint, Outlook, SQL Servers and DropBox which keeps its data primarily in Western Europe, it is ODEK's understanding that the aforementioned entities store their data in a compliant data centre and each entity is subject to binding laws which provide an adequate level of protection that is in line with POPIA;

7.4 ODEK will only be responsible for the privacy of data transmitted over the Internet using ODEK approved applications and transfer protocols and stored in ODEK approved data centres and storage devices. ODEK adheres to globally recognised best security practices with regards to protecting a data subjects' personal information. However, despite these preventative measures ODEK can't guarantee absolute security as the internet is an open system.

8. COMPLIANCE MONITORING

8.1. Policies will be monitored and updated on an annual basis;

8.2. Sampling will be done at regular intervals to test the Policy;

8.3. Consequences of non-compliance:

- Warning;
- Reporting of incidents to the relevant authorities;
- Reporting of incidents to relevant clients and/or users;
- Possible sanctions and regulatory fines.

9. RIGHTS OF DATA SUBJECTS

9.1 The right of access: The data subject may request that ODEK confirm that it holds the persons information and may request details of how the information is processed. The following procedure is set out in the ODEK PAIA Manual which may be requested via email to compliance@odek.co.za;

9.2 The right to rectification: The data subject may request ODEK to rectify or update incorrect personal information, by requesting same via email to compliance@odek.co.za;

9.3 The right to removal: Where there is no longer any legal basis or legitimate reason to process personal information and the FICA retention period has expired, the data subject may request that ODEK return or destroy any and all of the personal information in our possession or control, by requesting same via email to compliance@odek.co.za;

9.4 The right to object to, restrict further processing and withdraw consent: The data subject may at any point object, restrict the further processing of personal information or withdraw consent by requesting same via email to compliance@odek.co.za.

10. CHANGES TO THE POLICY AND GOVERNING LAW

10.1. ODEK reserves the right to amend or update this POPIA Policy at any time;

10.2. This Policy shall be governed by and interpreted in accordance with the laws of the Republic of South Africa, and the jurisdiction of the Courts of the Republic of South Africa;

10.3. The terms and conditions of this Policy are severable, in that if any provision is determined to be illegal or unenforceable by any Court of competent jurisdiction, such provision shall be deemed to have been deleted without affecting the remaining provisions of this Policy;

10.4. ODEK's failure to exercise any particular rights or provision of this Policy shall not constitute a waiver of such right or provision, unless acknowledged and agreed to by ODEK in writing.

11. CONTACT

If a client and/or user wishes to lay a complaint, obtain further clarity regarding this Policy, verify or update their information or request a copy of this Policy, they must address correspondence via email to compliance@odek.co.za and address same to Nadine dos Santos. Alternatively, they should contact the ODEK offices on 087 350 6335 from 8:00 – 17:00, Monday to Friday.

12. COMPLAINTS

12.1. All complaints will be treated in a confidential manner.

12.2. Should a client and/or user feel unsatisfied with the handling of their data, or about any complaint already made to ODEK, the complaint may then be escalated to the Information Regulator as follows:

Information Regulator of South Africa

Email: complaints.IR@justice.gov.za

Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001

P.O Box 31533 Braamfontein, Johannesburg