PROTECTION OF PERSONAL INFORMATION ACT OF 2013 MANUAL

This Manual and the Annexures thereto ensure the POPIA compliance of Koue Bokkeveld Training Centre (hereinafter "Koue Bokkeveld Training Centre")

THE ACT

In terms of the Constitution of South Africa, everyone has the right to privacy. This includes the right against unlawful collection, retention, dissemination and use of personal information. The Protection of Personal Information Act, 4 of 2013 therefore regulates the processing of such personal information by public and private bodies in a manner that gives effect to the constitutional right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests, particularly that of access to information.

The Act requires responsible parties to take actions to ensure protection of personal information when processing, and compliance with the eight lawful conditions of processing which will be outlined below.[1]

CONTENTS

[1] See Page 8

INTRODUCTION

This Data Protection and Information Sharing Manual describes the way that **Koue Bokkeveld Training Centre** will meet its legal obligations and requirements concerning confidentiality and information security standards. The requirements within the Policy are primarily based upon the Protection of Personal Information Act, No. 4 of 2013, as that is the key piece of legislation covering security and confidentiality of personal information.

Contact Details

Organisation: Koue Bokkeveld Training Centre

Information Officer: Carmen Lizelle Roberts (CEO)

Postal Address: PO Box 56, Op die Berg, Koue Bokkeveld

Physical Address: 63 Bergsig Street, Op die Berg, Koue Bokkeveld, 6836

Telephone Number: 0233170983 /0233170588

Email address: carmen@kbos.co.za

Role of the Information Officer[2]

Regulation 4 sets out several responsibilities for the Information Officer, in addition to that prescribed by POPIA, which include:

a) Developing, implementing, and monitoring a compliance framework for protection of personal information.
b) Ensuring that a personal information impact assessment is done to ensure that adequate measures and standards exist.
c) Developing, monitoring, maintaining and make available a manual, as prescribed by the Promotion of Access to Information Act, 2 of 2000.
d) Developing internal measures and systems to process requests for access to information.
e) Ensuring that internal awareness training sessions are conducted.

Registration of Information Officer[3]

Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator. The current Information officer has been registered. Should there be a change in Information officer, the particulars will be updated. The Information Officer and Deputy Information Officer acknowledges that the Regulator will make their contact details available on its website.

DEFINITIONS

The terms used in this manual and legislation are defined as follows:

"The Act": The Protection of Personal Information Act, 4 of 2013, and includes any regulation under this act.

''Automated means": any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

"Biometrics": A technique of personal identification that is based on physical, physiological, or behavioral characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

"Body": public or private body.

[2] Please use the guidance provided in Annexure 1 and ensure this is signed by the information officer and deputy information officer

[3] The address for the portal is https://justice.gov.za/inforeg/portal.html

"Child": 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.

"Code of conduct": A code of conduct issued by the Regulator in terms of Chapter 7 of the Act.

"Competent person": Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

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

"Constitution": The Constitution of the Republic of South Africa, 1996.

"Data subject": The person to whom personal information relates.

"De-identify": In relation to personal information of a data subject, means to delete any information that identifies the data subject, can be used or manipulated by a reasonably foreseeable method to identify the data subject, or can be linked by a reasonably foreseeable method to other information that identifies the data subject.

"Direct marketing": 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 data subject, or requesting the data subject to make a donation of any kind for any reason.

"Electronic communication": 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.

"Enforcement notice": A notice issued by the Regulator to a responsible party in order to take certain action.

"Filing system": Any structured set of information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

"Head": of, or in relation to, a private body means:

a) in the case of a natural person, that natural person or any person duly authorised by that natural person;
b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
c) in the case of a juristic person the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer;

"Information matching programme": The comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject.

"Minister": The Cabinet member responsible for the administration of justice.

"Operator": 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. This means that the information you process is not for your direct client, employee, supplier, etc. but rather that of another entity. For example, if you provide payroll services and as such process the information of another entity's employees.

"Person": A natural person or a juristic person.

"Personal information": 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, 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.

"POPI": Protection of Personal Information.

"POPIA": Protection of Personal Information Act

"PAIA": Promotion of Access to Information Act

"Prescribed": Prescribed by regulation or by a code of conduct.

"Private body":

a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
b) a partnership which carries or has carried on any trade, business or profession; or
c) any former or existing juristic person but excludes a public body.

"Processing": 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,
b) consultation or use;
c) dissemination by means of transmission, distribution or making available in any other form; or
d) merging, linking, as well as restriction, degradation, erasure or destruction of information.

"Professional legal adviser": Any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice.

"Public body":

a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
b) any other functionary or institution when:
    a. exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or
    b. exercising a public power or performing a public function in terms of any legislation.

"Public record": 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.

"Record": Any recorded information:

a) regardless of form or medium, including any of the following:
    a. Writing on any material;
    b. 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;
    c. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    d. book, map, plan, graph or drawing;
    e. 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;
b) in the possession or under the control of a responsible party;
c) whether or not it was created by a responsible party; and
d) regardless of when it came into existence.

"Regulator": The Information Regulator established in terms of section 39 of the Act.

"Re-identify": In relation to personal information of a data subject, means to resurrect any information that has been de-identified, 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, ''re-identified'' has a corresponding meaning.

"Republic": The Republic of South Africa.

"Responsible party": A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

"Restriction": 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.

"Special personal information":

a) 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
b) the criminal behaviour of a data subject to the extent that such information relates to:
   a. the alleged commission by a data subject of any offence; or
   b. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

"Third party/3rd party": facilitators, SETA's, and donors.

"Unique identifier": 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.

SCOPE OF THIS MANUAL

The Policy applies to all employees, directors, sub-contractors, agents, and appointees of Koue Bokkeveld Training Centre. The provisions of the manual are applicable to both on and off-site processing of personal information. Koue Bokkeveld Training Centre collects and uses Personal Information of the individuals and corporate entities with whom it works in order to operate and carry out its business effectively.

Koue Bokkeveld Training Centre regards the lawful and appropriate processing of all Personal Information as crucial to successful service delivery and essential to maintaining confidence between Koue Bokkeveld Training Centre and those individuals and entities who we deal it. Koue Bokkeveld Training Centre therefore fully endorses and adheres to the principles of the Protection of Personal Information Act.

PROCESSING OF PERSONAL INFORMATION

Purpose of Processing

Koue Bokkeveld Training Centre uses the Personal Information under its care in the following ways:

a) Record Keeping of all students trained
b) Reporting to relevant accreditation bodies
c) Reporting to funders
d) Administration of agreements
e) Providing products and services to customers
f) Detecting and prevention of fraud, crime, money laundering and other malpractice
g) Conducting market or customer satisfaction research
h) Marketing and sales
i) Staff administration
j) Keeping of accounts and records
k) Complying with legal and regulatory requirements
l) Profiling data subjects for the purposes of direct marketing

Categories of Data Subjects and their Personal Information[4]

Entity Type	Personal Information Processed
Clients/Customers: Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence; photo's, language, educational information
Clients/Customers: Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information; photo's
Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information; photo's
Employees / Directors / Owners	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being; photo's

Categories of Recipients for Processing the Personal Information

Koue Bokkeveld Training Centre may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services.

Koue Bokkeveld Training Centre may supply the Personal Information to any party to whom Koue Bokkeveld Training Centre may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

a) Capturing and organising of data
b) Storing of data
c) Sending of emails and other correspondence to customers
d) Conducting due diligence checks
e) Administration of training
f) The performance of contractual agreements
g) Hosting of our website / newsletters/ annual reports
h) Application, implementation and reporting of funding

Actual or Planned Transborder Flows of Personal Information

Personal Information may be transmitted trans-border to Koue Bokkeveld Training Centre's authorised dealers and its suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. Koue Bokkeveld Training Centre will endeavor to ensure that its dealers and suppliers will make all reasonable efforts to secure said data and Personal Information.

Retention of Personal Information Records

Koue Bokkeveld Training Centre may retain Personal Information records indefinitely unless the Data Subject objects thereto. If the Data Subject objects to indefinite retention of its Personal Information Koue Bokkeveld Training Centre shall retain the Personal Information records to the extent permitted or required by law.

[4] These data subjects must be copied from Annexure 3.

General Description of Information Security Measures

Koue Bokkeveld Training Centre employs up to date technology to ensure the confidentiality, integrity and availability of the Personal Information under its care. Measures include:

a) Firewalls
b) Virus protection software and update protocols
c) Logical and physical access control
d) Secure setup of hardware and software making up the IT infrastructure
e) Outsourced Service Providers who process Personal Information on behalf of Koue Bokkeveld Training Centre are contracted to implement security controls.

ACCESS TO PERSONAL INFORMATION

All individuals and entities may request access, amendment, or deletion of their own Personal Information held by Koue Bokkeveld Training Centre. Any requests should be directed, on the prescribed form, to the Information Officer.

Remedies available if request for access to Personal Information is refused:

Internal Remedies

Follow internal appeal procedures as stipulated in the KBOS policy. As such, the decision made by the Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

External Remedies

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for relief. Likewise, a third party dissatisfied with the information officer's decision to grant a request for information, may within 30 days of notification of the decision, apply to a court for relief. For purposes of the Act, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status.

Grounds for Refusal

Koue Bokkeveld Training Centre may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds on which Koue Bokkeveld Training Centre may refuse access include:

a) Protecting personal information that Koue Bokkeveld Training Centre holds about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;
b) Protecting commercial information that Koue Bokkeveld Training Centre holds about a third party or Koue Bokkeveld Training Centre (for example trade secret: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);
c) If disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;
d) If disclosure of the record would endanger the life or physical safety of an individual;
e) If disclosure of the record would prejudice or impair the security of property or means of transport;
f) If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;
g) If disclosure of the record would prejudice or impair the protection of the safety of the public;
h) The record is privileged from production in legal proceedings, unless the legal privilege has been waived;
i) Disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information)

would harm the commercial or financial interests of Koue Bokkeveld Training Centre;

j) Disclosure of the record would put Koue Bokkeveld Training Centre at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;

k) The record is a computer programme; and

l) The record contains information about research being carried out or about to be carried out on behalf of a third party or Koue Bokkeveld Training Centre.

Records that cannot be found or do not exist

If Koue Bokkeveld Training Centre has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

IMPLEMENTATION GUIDELINES

Training & Dissemination of Information[5]

a) Training on the Policy and POPI at Koue Bokkeveld Training Centre will take place with all affected employees.

b) All new employees will be made aware at induction, or through training programmes, of their responsibilities under the terms of this Policy and POPI

c) Modifications and updates to data protection and information sharing policies, legislation, or guidelines will be brought to the attention of all staff.

Employee Contracts

a) Each new employee will sign an Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

b) Each employee currently employed within Koue Bokkeveld Training Centre will sign an addendum to their Employment Contract containing the relevant consent clauses for the use and storage of employee information, and a confidentiality undertaking as part and will be personally responsible for ensuring there are no breaches of confidentiality in relation to any Personal Information, however it is stored. Failure to comply will result in the instigation of a disciplinary procedure.

EIGHT PROCESSING CONDITIONS

POPI is implemented by abiding by eight processing conditions. Koue Bokkeveld Training Centre shall abide by these principles in all its processing activities.

Accountability

Koue Bokkeveld Training Centre shall ensure that all processing conditions, as set out in POPI, are complied with when determining the purpose and means of processing Personal Information and during the processing itself. Koue Bokkeveld Training Centre shall remain liable for compliance with these conditions, even if it has outsourced it processing activities.

[5] Not everyone needs to be trained on the full impact of the act. Most employees only need to be aware of how this impact on their day-to-day activities. Existing employees – Internal workshops and discussions on specific requirements and responsibilities to be held at least once a year) and formal training will be utilized if necessary.

Processing Limitation

Lawful grounds for the processing of Personal Information are the key elements. The processing of Personal Information is only lawful if, given the purpose of processing, the information is adequate, relevant and not excessive. Koue Bokkeveld Training Centre may only process Personal Information if one of the following grounds of lawful processing exists:

a) The Data Subject consents to the processing;
b) Processing is necessary for the conclusion or performance of a contract with the Data Subject;
c) Processing complies with a legal responsibility imposed on Koue Bokkeveld Training Centre;
d) Processing protects a legitimate interest of the Data Subject;
e) Processing is necessary for pursuance of a legitimate interest of Koue Bokkeveld Training Centre, or a third party to whom the information is supplied;

Special Personal Information includes:

a) Religious, philosophical, or political beliefs;
b) Race or ethnic origin;
c) Trade union membership;
d) Health or sex life;
e) Biometric information (including blood type, fingerprints, DNA, retinal scanning, voice recognition, photographs);
f) Criminal behaviour;
g) Information concerning a child.

Koue Bokkeveld Training Centre may only process Special Personal Information under the following circumstances:

a) The Data Subject has consented to such processing;
b) The Special Personal Information was deliberately made public by the Data Subject;
c) Processing is necessary for the establishment of a right or defence in law;
d) Processing is for historical, statistical, or research reasons
e) If processing of race or ethnic origin is in order to comply with affirmative action laws

All Data Subjects have the right to refuse or withdraw their consent to the processing of their Personal Information, and a Data Subject may object, at any time, to the processing of their Personal Information on any of the above grounds, unless legislation provides for such processing. If the Data subject withdraws consent or objects to processing then Koue Bokkeveld Training Centre shall forthwith refrain from processing the Personal Information.

Collection directly from the Data Subject

Personal Information must be collected directly from the Data Subject, unless:

a) Personal Information is contained in a public record;
b) Personal Information has been deliberately made public by the Data Subject;
c) Personal Information is collected from another source with the Data Subject's consent;
d) Collection of Personal Information from another source would not prejudice the Data Subject;
e) Collection of Personal Information from another source is necessary to maintain, comply with or exercise any law or legal right;
f) Collection from the Data Subject would prejudice the lawful purpose of collection;
g) Collection from the Data Subject is not reasonably practicable.

Purpose Specification

Koue Bokkeveld Training Centre shall only process Personal Information for the specific purposes as set out and defined above at paragraph 5.1.

Further Processing

New processing activity must be compatible with original purpose of processing. Further processing will be regarded as compatible with the purpose of collection if:

a) Data Subject has consented to the further processing;
b) Personal Information is contained in a public record;
c) Personal Information has been deliberately made public by the Data Subject;
d) Further processing is necessary to maintain, comply with or exercise any law or legal right;
e) Further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or a third party

Information Quality

Koue Bokkeveld Training Centre shall take reasonable steps to ensure that Personal Information is complete, accurate, not misleading and updated. Koue Bokkeveld Training Centre shall periodically review Data Subject records to ensure that the Personal Information is still valid and correct.

Employees should as far as reasonably practical follow the following guidance when collecting Personal Information:

a) Personal Information should be dated when received;
b) A record should be kept of where the Personal Information was obtained;
c) Changes to information records should be dated;
d) Irrelevant or unneeded Personal Information should be deleted or destroyed;
e) Personal Information should be stored securely, either on a secure electronic database or in a secure physical filing system.

Openness

Koue Bokkeveld Training Centre shall take reasonable steps to ensure that the Data Subject is made aware of:

a) What Personal Information is collected, and the source of the information;
b) The purpose of collection and processing;
c) Where the supply of Personal Information is voluntary or mandatory, and the consequences of a failure to provide such information;
d) Whether collection is in terms of any law requiring such collection;
e) Whether the Personal Information shall be shared with any third party.

Data Subject Participation

Data Subjects have the right to request access to, amendment, or deletion of their Personal Information.

All such requests must be submitted in writing to the Information Officer. Unless there are grounds for refusal as set out above[6], Koue Bokkeveld Training Centre shall disclose the requested Personal Information:

On receipt of adequate proof of identity from the Data Subject, or requester;

a) Within a reasonable time;
b) On receipt of the prescribed fee, if any;
c) In a reasonable format

[6] See ACCESS TO PERSONAL INFORMATION: Grounds for refusal

Koue Bokkeveld Training Centre shall not disclose any Personal Information to any party unless the identity of the requester has been verified.

Security Safeguards

Koue Bokkeveld Training Centre shall ensure the integrity and confidentiality of all Personal Information in its possession, by taking reasonable steps to:

a) Identify all reasonably foreseeable risks to information security;
b) Establish and maintain appropriate safeguards against such risks;

Written records

a) Personal Information records should be kept in locked cabinets, or safes;
b) When in use Personal Information records should not be left unattended in areas where non-staff members may access them;
c) Koue Bokkeveld Training Centre shall implement and maintain a "Clean Desk Policy" where all employees shall be required to clear their desks of all Personal Information when leaving their desks for any length of time and at the end of the day;
d) Personal Information which is no longer required should be disposed of by shredding.
e) Any loss or theft of, or unauthorised access to, Personal Information must be immediately reported to the Information Officer.

Electronic Records

a) All electronically held Personal Information must be saved in a secure database;
b) As far as reasonably practicable, no Personal Information should be saved on individual computers, laptops or hand-held devices;
c) All computers, laptops and hand-held devices should be access protected with a password, fingerprint or retina scan, with the password being of reasonable complexity and changed frequently;
d) Koue Bokkeveld Training Centre shall implement and maintain a "Clean Screen Policy" where all employees shall be required to lock their computers or laptops when leaving their desks for any length of time and to log off at the end of the day;
e) Electronical Personal Information which is no longer required must be deleted from the individual laptop or computer and the relevant database. The employee must ensure that the information has been completely deleted and is not recoverable.
f) Any loss or theft of computers, laptops or other devices which may contain Personal Information must be immediately reported to the Information Officer, who shall notify the IT department, who shall take all necessary steps to remotely delete the information, if possible.

DIRECT MARKETING

All Direct Marketing communications shall contain Koue Bokkeveld Training Centre's, and/or the Company's (if Applicable) details, and an address or method for the customer to opt-out of receiving further marketing communication.

Existing Customers

Direct Marketing by electronic means to existing customers is only permitted:

a) If the customer's details were obtained in the context of a sale or service; and
b) For the purpose of marketing the same or similar products;

c) The customer must be given the opportunity to opt-out of receiving direct marketing on each occasion of direct marketing.

Consent

Koue Bokkeveld Training Centre may send electronic Direct Marketing communication to Data Subjects who have consented to receiving it. Koue Bokkeveld Training Centre may approach a Data Subject for consent only once.

Record Keeping

Koue Bokkeveld Training Centre shall keep record of:

a) Date of consent
b) Wording of the consent
c) The person who obtained consent
d) Proof of opportunity to opt-out on each marketing contact
e) Record of opt-outs

PROMOTION OF ACCESS TO INFORMATION ACT

A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act. The head of a private body[7] must make a manual available containing:

a) in general:
   a. the postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;
   b. such other information as may be prescribed;
b) insofar as PAIA is concerned:
   a. description of the guide of how to use the PAIA as referred to in section 10, if available, and how to obtain access to it;
   b. the latest notice, if any, regarding the categories of records of the body which are available without a person having to request access in terms of PAIA;
   c. a description of the records of the body which are available in accordance with any other legislation;
   d. sufficient detail to facilitate a request for access to a record of the body, a description of the subjects on which the body holds records and the categories of records held on each subject;
c) insofar as the Protection of Personal Information Act, 2013, is concerned:
   a. the purpose of the processing;
   b. a description of the categories of data subjects and of the information or categories of information relating thereto;
   c. the recipients or categories of recipients to whom the personal information may be supplied;
   d. planned trans-border flows of personal information; and
   e. a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

The head of a private body must on a regular basis update the manual.

The manual must be made available:

[7] Please delete if you are a public body.

d) on the website, if any, of the private body;

e) at the principal place of business of the private body for public inspection during normal business hours;

f) to any person upon request and upon the payment of a reasonable amount; and

g) to the Information Regulator upon request.

The minister has exempted all private bodies from compiling the manual until 31 December 2020 except for companies which:

a) Is not a private company as defined in section 1 of the Companies Act, 2008 (Act 71 of 2008); and
b) Is a private company as defined in section 1 of the Companies Act, 2008 (Act 71 of 2008) which operates within any of the sectors mentioned in column one of the Schedule and:
   a) Has 50 or more employees in their employment; or
   b) Has a total annual turnover that is equal to or more than the applicable amount mentioned in column 2 of the Schedule to this Notice.

Column 1	**Column 2**
Agriculture	R 6 million
Mining and quarrying	R 22.5 million
Manufacturing	R 30 million
Electricity, gas and water	R 30 million
Construction	R 15 million
Retail and motor trade and repair services	R 45 million
Wholesale trade, commercial agents and allied services	R 75 million
Catering, accommodation and other trade	R 15 million
Transport, storage and communications	R 30 million
Finance and business services	R 30 million
Community, special and personal services	R 15 million

DESTRUCTION OF DOCUMENTS

Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Koue Bokkeveld Training Centre pending such return.

The documents must made available for collection by an approved document disposal company.

Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

STATUTORY RETENTION PERIODS

Document Type	Period

Companies Act	
a) Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; b) Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; c) Copies of reports presented at the annual general meeting of the company; d) Copies of annual financial statements required by the Act; e) Copies of accounting records as required by the Act; f) Record of directors and past directors, after the director has retired from the company; g) Written communication to holders of securities and h) Minutes and resolutions of directors' meetings, audit committee and directors' committees.	7 Years
a) Registration certificate; b) Memorandum of Incorporation and alterations and amendments; c) Rules; d) Securities register and uncertified securities register; e) Register of company secretary and auditors and f) Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.	Indefinitely
Consumer Protection Act	
a) Full names, physical address, postal address and contact details; b) ID number and registration number; c) Contact details of public officer in case of a juristic person; d) Service rendered; e) Cost to be recovered from the consumer; f) Frequency of accounting to the consumer; g) Amounts, sums, values, charges, fees, remuneration specified in monetary terms; h) Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;	3 years
Financial Intelligence Centre Act	
d) Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer; e) If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person; f) If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer; g) The manner in which the identity of the persons referred to above was established;	5 years

h) The nature of that business relationship or transaction; i) In the case of a transaction, the amount involved and the parties to that transaction; j) All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction; k) The name of the person who obtained the identity of the person transacting on behalf of the accountable institution; l) Any document or copy of a document obtained by the accountable institution	
Compensation for Occupational Injuries and Diseases Act	
a) Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
Section 20(2) documents: a) Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; b) Records of incidents reported at work.	3 years
Asbestos Regulations, 2001, regulation 16(1): a) Records of assessment and air monitoring, and the asbestos inventory; b) Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): a) Records of risk assessments and air monitoring; b) Medical surveillance records. Lead Regulations, 2001, Regulation 10: a) Records of assessments and air monitoring; b) Medical surveillance records Noise - induced Hearing Loss Regulations, 2003, Regulation 11: a) All records of assessment and noise monitoring; b) All medical surveillance records, including the baseline audiogram of every employee.	40 years
Hazardous Chemical Substance Regulations, 1995, Regulation 9: a) Records of assessments and air monitoring; b) Medical surveillance records	30 years
Basic Conditions of Employment Act	
Section 29(4): a) Written particulars of an employee after termination of employment; Section 31: a) Employee's name and occupation; b) Time worked by each employee; c) Remuneration paid to each employee;	3 years

d) Date of birth of any employee under the age of 18 years.	
Employment Equity Act	
a) Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; b) Section 21 report which is sent to the Director General	3 years
Labour Relations Act	
a) 3 years	3 years
a) An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; b) Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
Unemployment Insurance Act	
Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.	5 years
Tax Administration Act	
Section 29 documents which: a) Enable a person to observe the requirements of the Act; b) Are specifically required under a Tax Act by the Commissioner by the public notice; c) Will enable SARS to be satisfied that the person has observed these requirements	5 years
Income Tax Act	
a) Amount of remuneration paid or due to the employee; b) The amount of employee's tax deducted or withheld from the remuneration paid or due; c) The income tax reference number of that employee; d) Any further prescribed information; Employer Reconciliation return.	5 years
Value Added Tax Act	
a) Where a vendor's basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period; b) Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; c) Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; d) Documentary proof substantiating the zero rating of supplies; e) Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	5 years

ANNEXURES

a) Form 1: Initial Letter to Client
b) Form 2: Clients consent to process personal information
c) Form 3: Objection to processing of personal information
d) Form 4: Request for correction or deletion of personal information
e) Form 5: Application for consent to direct marketing
f) Form 6: Addendum to the Service Agreement or Letter of Appointment
g) Form 7: Information Officer's registration form
h) Form 8: Designation and delegation to Deputy Information Officer
i) Form 9: Authorisation of Information Officer