# Protection of Personal Information, Information Security and Records Management Policy

## Privacy is Paramount

This is the **Protection of Personal Information, Information Security and Records Management Policy** for

**QED Actuaries and Consultants (Pty) Limited, Registration number: 1991/005277/07**

**QED South Africa (Pty) Limited, Registration number: 2018/612863/07**

**QED Employee Benefits (Pty) Limited, Registration number: 2018/630030/07**

**QED Holding Company (Pty) Limited, Registration number: 1999/012144/07**

(collectively referred to as the "**Organisation**")

Note: This document serves as the internal POPI or Privacy Policy of QED. It is a summary of the PAIA and POPI Manual. It is recommended that this document is also uploaded onto the QED website and that every employee within QED is provided with a copy. It should form part of QED's other internal policies and procedures and should be implemented accordingly.

# Protection Of Personal Information In Terms Of The Protection Of Personal Information Act 4 Of 2013

## 1. Introduction

1.1 The Organisation is a consulting company providing actuarial services to clients. This requires the Organisation to collect, collate, store, and disseminate a vast amount of personal information on a daily basis, obliging the Organisation to comply with the Protection of Personal Information Act 4 of 2013 ("**Act**").

1.2 The Act requires the Organisation to inform their clients as to the manner in which their personal information is used, disclosed, and destroyed. The Organisation is committed to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

1.3 This Policy sets out the manner in which the Organisation deals with their client's personal information as well as stipulates the purpose for which said information is used.

1.4 This Policy is made available at the Organisation's registered address and by request from the Organisation.

1.5 This Policy is drafted in conjunction with the National Credit Act 34 of 2005, and the Consumer Protection Act 68 of 2008.

## 2. Background And Purpose

### 2.1 What Is The Purpose Of The Act (POPIA)?

2.1.1 The aim of the Act is to ensure the right of South African citizens to the privacy of personal information and to regulate all organisations that collect, store, and disseminate personal information.

2.1.2 Personal information may only be processed if the process meets the conditions of the Act.

2.1.3 There are **8 (eight) distinct conditions** which organisations need to meet to be acting lawfully:

**2.1.3.1 accountability;**

**2.1.3.2 processing limitation;**

**2.1.3.3 purpose specification;**

**2.1.3.4 use limitation;**

**2.1.3.5 information quality;**

**2.1.3.6 openness;**

**2.1.3.7 security safeguards; and**

**2.1.3.8 individual/data subject participation.**

### 2.2 What Is "Personal Information"?

2.2.1 Personal information means any information relating to an identifiable natural person (and existing juristic persons where applicable), including information relating to:

2.2.1.1 race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, belief, culture, language, and birth;

2.2.1.2 education, medical, financial, criminal or employment;

2.2.1.3 identity number, electronic and physical addresses, telephone numbers and on-line identifiers;

2.2.1.4 biometric information;

2.2.1.5 personal opinions, views, or preferences; and,

2.2.1.6 correspondence sent by a person implicitly or explicitly of a personal nature or confidential.

2.2.2 An organisation may not process the personal information of a child (under 18 years) unless the processing:

2.2.2.1 is carried out with the consent of the legal guardian;

2.2.2.2 is necessary to establish, exercise or defence of a right or obligation in law;

2.2.2.3 is necessary for historical, statistical or research purposes; or,

2.2.2.4 is information that is deliberately been made public by the child with the consent of the guardian.

## 2.3 What Is Processing Personal Information?

2.3.1 Processing means any operation or activity, or set of activities, by automatic means or otherwise, including:

2.3.1.1 collecting, receiving, recording, collating, storing, updating, modifying, retrieving or use;

2.3.1.2 disseminating by means of transmission, distribution, or any other means; or,

2.3.1.3 merging, linking, restricting, erasing, or destructing of information.

## 2.4 Who Must Comply?

2.4.1 All public and private bodies (natural and juristic persons) must comply.

## 2.5 What Does Compliance Mean?

### 2.5.1 Accountability

2.5.1.1 Organisations must assign responsibility to ensure compliance with the Act to a suitable person or persons.

2.5.1.2 Each organisation has an "**information officer**." This will be the same person who has been appointed by the organisation as head in terms of the Promotion of Access to Information Act, i.e. the CEO or equivalent.

2.5.1.3 The information officer, together with an executive team/board, should decide on and record the POPI policy and procedure (this policy).

2.5.1.4 The information officer must appoint a "data controller" or a number of data controllers who decide:

2.5.1.4.1 the purpose of the data processing; and,

2.5.1.4.2 the way the personal information should be processed.

2.5.1.5 The data controllers should be Management who execute the POPI policy and procedure.

2.5.1.6 "Data processor/s" perform the processing administration/function (e.g. data capturing etc).

### 2.5.2 Processing Limitation

2.5.2.1 Personal information may only be processed if it is:

2.5.2.1.1 adequate, relevant, and necessary for the purpose for which it is processed;

2.5.2.1.2 with the consent of the data subject;

2.5.2.1.3 necessary for the contract to which the data subject is party;

2.5.2.1.4 necessary for the protection of a legitimate interest of the data subject;

2.5.2.1.5 required by law;

2.5.2.1.6 necessary to pursue the legitimate interest of the organisation; or,

2.5.2.1.7 collected directly from the data subject, except in certain circumstances (e.g. in public domain or to do so would defeat the purpose for collecting and processing).

2.5.2.2 "**Consent**" must be:

2.5.2.2.1 voluntary;

2.5.2.2.2 specific; and,

2.5.2.2.3 informed.

2.5.2.3 Informed consent requires that the data subject understand:

2.5.2.3.1 what information is being collected/processed;

2.5.2.3.2 why the information is being processed;

2.5.2.3.3 how the information is to be processed;

2.5.2.3.4 where the information is being processed; and,

2.5.2.3.5 to whom the information is intended to be given.

### 2.5.3 Purpose Specification

2.5.3.1 The data subject must be made aware of the purpose for which the information is being collected ("identified purpose"). This is necessary for giving consent (see above).

### 2.5.4 Use Limitation

2.5.4.1 Information/records may only be kept for as long as it is necessary to achieve the identified purpose. There are some statutory record-keeping periods which may exceed this.

2.5.4.2 After this retention period the responsible person must delete or destroy such information as soon as reasonably possible.

2.5.4.3 If the purpose changes (e.g. something else occurs that could use the same information again for this alternative purpose), it may be necessary to inform the data subject and get consent again.

### 2.5.5 Information Quality

2.5.5.1 Information must be as accurate as possible, complete, and updated if necessary.

2.5.5.2 Information must be available to the data subject to verify/object to the accuracy thereof.

### 2.5.6 Openness

2.5.6.1 The Organisation must take reasonable practical steps to ensure that the data subject is aware of what personal information is being collected, stored, and used, whether or not collected directly from the data subject.

### 2.5.7 Security Safeguards

2.5.7.1 The organisation must secure the integrity and confidentiality of personal information und must take appropriate technical/organisational measure to prevent:

2.5.7.1.1 the loss of or damage to personal information; or,

2.5.7.1.2 the unlawful access to or processing of personal information.

2.5.7.2 To do this, the organisation must:

2.5.7.2.1 identify all reasonable, foreseeable, internal, and external risks to personal information held;

2.5.7.2.2 establish and maintain appropriate reasonable safeguards against the risks;

2.5.7.2.3 monitor the safeguards and regularly verify safeguards are effective; and,

2.5.7.2.4 ensure safeguards are updated to respond to new risks or deficiencies in previous safeguards.

2.5.7.3 The data controllers and data processors must operate under his/her authority from the information officer and treat all personal information as confidential.

2.5.7.4 Where there are reasonable grounds for suspecting a breach of data security, the responsible person must notify the Regulator and the data subject.

### 2.5.8 Data Subject Participation

2.5.8.1 Any person who can positively identify themselves is entitled to access their own personal information.

2.5.8.2 A data subject has the right to correct or amend any of their personal information that may be inaccurate, misleading, or out of date.

## 2.6 What Steps Should Be Taken To Comply?

2.6.1 An audit should be conducted of the following:

2.6.1.1 what personal information is held?

2.6.1.2 where the personal information is being held?

2.6.1.3 by whom is the personal information being held?

2.6.2 Establish what personal information is being collected in one place and being transferred to another.

2.6.3 Review privacy statements, email indemnity, supplier or other standard terms and conditions, engagement letters, employee letters of appointment and third-party agreements that will process personal information of your clients or customers.

2.6.4 Develop organisation wide standard data protection policies and protocols, and if in place already in place, review such policies and protocols.

2.6.5 Review IT outsourcing contracts and arrangements.

2.6.6 Review data collecting activities (completion of forms etc).

2.6.7 Appoint an information officer for POPI and PAIA purposes.

2.6.8 Provide training to staff.

## 2.7 Details of Information Officer and Deputy Information Officer

2.7.1 The details of the Organisation's Information Officer and Deputy Information Officer are as follows:

| | |
|---|---|
| **Information Officer:** | Craig Falconer |
| **Address:** | 1st Floor, The Bridle, Hunts End Office Park, 38 Wierda Road West, Sandton, 2196 |
| **Telephone Number:** | +27 11 038 3700 |
| **E-mail:** | craig.falconer@qedact.com |

| | |
|---|---|
| **Deputy Information Officer:** | Etienne Louw |
| **Address:** | 1st Floor, The Bridle, Hunts End Office Park, 38 Wierda Road West, Sandton, 2196 |
| **Telephone Number:** | +27 11 038 3700 |
| **E-mail:** | etienne.louw@qedact.com |

## 3. Personal Information Collected

3.1 Section 9 of the Act states that "**Personal Information**" may only be processed if, given the purpose for which it is processed, it is adequate, relevant, and not "**excessive**."

3.2 The Organisation collects and processes client's personal information for the following reasons:

3.2.1 to render the services requested;

3.2.2 to communicate with clients;

3.2.3 to market product offerings to clients;

3.2.4 for invoicing purposes;

3.2.5 confirming, verifying, and updating client details;

3.2.6 conducting market or customer satisfaction research;

3.2.7 internal HR purposes; and,

3.2.8 in connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

3.3 The type of information will depend on the need for which it is collected and will be processed for that purpose only.

**Note: Please provide us with only such information that we request. Where the Personal Information of a third party is required same will specifically be asked from you and will then be Processed in accordance with the terms contained herein.**

3.4 The data subject must ensure that where it provides the Organisation with Personal Information it shall at all times ensure that it has the necessary consents in place to share such Personal Information with the Organisation, specifically where the Personal Information of third parties is shared with the Organisation. An Operator Agreement will then be entered into between the Organisation and the data subject before such Personal Information will be processed by the Organisation.

3.5 The Organisation will always specify the Personal Information it will require from a data subject. Where Personal Information is shared with the Organisation that was not requested the Organisation shall immediately inform the data subject of such disclosure and will return and/or destroy such Personal Information it received.

3.6 The data subject shall regardless of the fact that the data subject had the consent to share such Personal Information in place or not, indemnify and keep the Organisation indemnified against any claims, damages, costs, or expenses that the Organisation may incur as a result of such unauthorised disclosure by a data subject.

3.7 Whenever possible, the Organisation will inform the client as to the information required and the information deemed optional.

3.8 The Organisation also collects and processes the client's personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

3.9 The Organisation aims to have agreements in place with all product suppliers and third-party service providers to ensure a mutual understanding with regard to the protection of the client's personal information. The Organisation suppliers will be subject to the same regulations as applicable to the Organisation.

3.10 With the client's consent, the Organisation may also supplement the information provided with information the Organisation receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with the Organisation. For purposes of this Policy, clients include potential and existing clients.

## 4. The Use Of Personal Information

4.1 The client's personal information will only be used for the purpose for which it was collected as set out in more detail under Clause 3.2 and as agreed to.

4.2 According to Section 10 of the Act, personal information may only be processed if certain conditions, listed below, are met along with supporting information for the Organisation processing of Personal Information:

4.2.1 the client's consent to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;

4.2.2 the necessity of processing: in order to conduct an accurate analysis of the client's needs;

4.2.3 processing complies with an obligation imposed by law on the Organisation;

4.2.4 to conduct an affordability assessment if applicable;

4.2.5 processing protects a legitimate interest of the client; or,

4.2.6 processing is necessary for pursuing the legitimate interests of the Organisation or of a third party to whom information is supplied.

## 5. Disclosure Of Personal Information

5.1 The Organisation may disclose a client's personal information to any of the Organisation subsidiaries, joint venture companies and or approved product supplier or third-party service providers whose services or products clients elect to use. The Organisation has agreements in place to ensure compliance with confidentiality and privacy conditions.

5.2 The Organisation may also share client personal information with and obtain information about clients from third parties for the reasons already discussed above.

5.3 The Organisation may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the Organisation rights.

5.4 All employees have a duty of confidentiality in relation to the Organisation and clients.

5.5 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of the Law. Information may be given to a third party if the client has consented in writing to that person receiving the information.

5.6 The Organisation views any contravention of this Policy very seriously and employees who are guilty of contravening the Policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

## 6. Safeguarding Personal Information

6.1 It is a requirement of the Act to adequately protect personal information. The Organisation will continuously review its security controls and processes to ensure that personal information is properly safeguarded.

6.2 The Organisation Information Officer is responsible for the compliance of the conditions of the lawful processing of personal information and other provisions of the Act. The Information Officer will be assisted by Deputy Information Officer/s.

6.3 This policy has been put in place throughout the Organisation and training on this policy and the Act has already taken place and will continue to be conducted by the Organisation.

6.4 Each new employee will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.

6.5 Every employee currently employed within the Organisation will be required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.

6.6 All the Organisation's electronic files or data are backed and stored off-site.

6.7 The Organisation's product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

## 7. Correction Of Personal Information

7.1 Clients have the right to access the personal information the Organisation holds about them. Clients also have the right to ask the Organisation to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, the Organisation may no longer process said personal information.

7.2 The Organisation will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

## 8. Amendments To This Policy

8.1 Amendments to, or a review of this Policy, will take place on an ad-hoc basis or at least once a year.

## 9. Access To Documents

9.1 All company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:

9.1.1 where disclosure is under compulsion of law;

9.1.2 where there is a duty to the public to disclose;

9.1.3 where the interests of the Organisation require disclosure; or

9.1.4 where disclosure is made with the express or implied consent of the client.

## 10. Requests For The Organisation Information

10.1 This is dealt with in terms of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Organisation, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

10.2 In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party has to state the reason for wanting the information and has to pay a prescribed fee.

10.3 The Organisation's manuals in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available from the Organisation.

10.4 Confidential company and/or business information of the Organisation may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Organisation must be kept strictly confidential at all times.

## 11. Retention Of Documents

11.1 **Hard Copy:** The statutory periods for the retention of documents are as per the Law. These are available on request.

11.2 **Electronic Storage:** The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage, and retrieval thereof. This will be done in conjunction with the departments concerned.

11.3 **Scanned Documents:** If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

11.4 Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes, or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.

11.5 It is also required that all personal information which has become obsolete must be destroyed.

## 12. Destruction Of Documents

12.1 Documents may be destroyed after the termination of the retention period specified in terms of the Law. Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

12.2 Each department is responsible for attending to the destruction of its documents, 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 Organisation pending such return.

12.3 After completion of the process in Clause 12.2 above, the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by the Organisation.

12.4 The documents are then made available for collection by the removers of the Organisation's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

12.5 Documents may also be stored off-site, in storage facilities approved by the Organisation.

## 13. Cross-Border Flows Of Personal Information

13.1 Section 72 of the Act provides that Personal Information may only be transferred out of the Republic of South Africa if the:

13.1.1 recipient country can offer such data an "adequate level" of protection. This means that its data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in the Act; or

13.1.2 the client or customer consents to the transfer of their personal information; or

13.1.3 transfer is necessary for the performance of a contractual obligation between the client or customer and the Organisation; or

13.1.4 transfer is necessary for the performance of a contractual obligation between the Organisation and a third party, in the interests of the client or customer; or

13.1.5 the transfer is for the benefit of the client or customer, and it is not reasonably practicable to obtain the consent of the client or customer, and if it were, the client or customer, would in all likelihood provide such consent.

13.2 The Organisation plans cross-border transfer of Personal Information to Mauritius, Nigeria, and Kenya. The same terms and conditions that is contained herein will apply thereto, unless in-country legislation provides for an alternative, more stringent method of dealing with Personal Information, in which case such in country legislation shall be followed.

| | |
|---|---|
| **Document Owner:** | InkLegal (Pty) Limited |
| **Approved by:** | Craig Falconer |
| **Date approved:** | August 2021 |
| **Due for review by Owner:** | August 2022 |
| **Version:** | 1 |