DATA PROTECTION POLICY

1. INTRODUCTION

The right to privacy is an integral human right recognised and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner. A person's right to privacy entails having control over his or her personal information and being able to conduct their affairs relatively free from unwanted intrusions.

Through the provision of quality financial services, EthiQal is involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees and other stakeholders.

Given the importance of privacy, EthiQal is committed to effectively managing personal information in accordance with the provisions of POPIA. Accordingly, the board of directors have endorsed the following Privacy Policy to be implemented throughout EthiQal its affiliates and subsidiaries.

Objectives, Scope, Policy Statement and Key Risks	
Objectives of policy	The objective of this policy is to ensure compliance with the Electronic Communications and Transaction Act 25 of 2002 and the Protection of Personal Information Act 4 of 2013 by setting out EthiQal's strategy to uphold the rights to privacy and confidentiality of personal information of its employees, policyholders and potential policyholders. The purpose of this policy is to enable EthiQal to: • Comply with the law in respect of the data it holds about individuals. • Follow industry best practice. • Protect EthiQal's staff policyholders and potential policy holders • Protect EthiQal from the consequences of non-compliance.
Scope of policy	This policy applies to the business of EthiQal wherever it is conducted. This Policy applies to: EthiQal's governing body. All branches, business units and divisions of the organisation. All employees and volunteers. All contractors, suppliers and other persons acting on behalf of the organisation.

	The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the organisation's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).
Policy statement	EthiQal will: • Comply with both the law and best practice. • Respect individuals' rights. • Be open and honest with individuals whose data is held. • Provide training and support for staff who handle personal data, so that they can act confidently and consistently. EthiQal recognises that a priority under the POPI Act is to avoid causing harm to individuals either directly or through inaction. In the main this means: • Retaining personal data and information securely. • Retention of good quality personal information. The Act aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are considered. EthiQal will comply with the Act in this respect. In addition to being open and transparent, EthiQal will seek to give individuals as much choice as is reasonably possible over what data is retained, for how long, and how it is used by EthiQal.
Key risks	EthiQal has identified the following potential key risks, which this policy is designed to address: • Breach of confidentiality (information being given out inappropriately) and accordingly non-compliance with the Act. • Insufficient clarity about the range of data usage leading to Data Subjects being insufficiently informed. • Failure to offer choice about data use when appropriate. • Breach of security by allowing unauthorised access. • Harm to individuals if personal data is not up to date. • Data Operator contracts failing to meet the minimum standards set out by the Act.

2. OVERVIEW OF DEFINITIONS, RIGHTS OF DATA SUBJECTS AND GENERAL GUIDING PRINCIPLES

Rights of Data Subjects	Refer to Annexure A
Definition of Personal Information	This policy applies to information relating to identifiable individuals, in terms of the Protection of Personal Information Act, 2013 (hereinafter POPI Act). Personal information is any information that can be used to reveal a person's identity. Personal information relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person (such as a company), including, but not limited to information concerning: • Race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth ofa person. • Information relating to the education or the medical, financial, criminal or employment history of the person. • Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person. • The biometric information of the person. • The personal opinions, views or preferences of the person. • Correspondence sent by the person that is implicitly or explicitly ofa private or confidential nature or further correspondence that would reveal the contents of the original correspondence. • The views or opinions of another individual about the person. • The name of the person if it appears with other personal information relating to the person or if the disclosure of the nameitself would reveal information about the person.

GENERAL GUIDING PRINCIPLES All employees and persons acting on behalf of EthiQal will always be subject to, and act in accordance with, the following guiding principles:	
Accountability	**Key Risk**: Failing to comply with POPIA could potentially damage EthiQal's reputation or expose EthiQal to a civil claim for damages or sanctionfrom the industry regulators. The protection of personal information is therefore everybody's responsibility. EthiQal will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of a compliance culture within the organisation. EthiQal will take appropriate sanctions, which may include disciplinary action, against those individuals who through theirintentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.
Processing Limitation	EthiQal will ensure that personal information under its control is processed: • In a fair, lawful and non-excessive manner. • Only with the informed consent of the data subject. • Only for a specifically defined purpose. EthiQal will inform the data subject of the reasons for collecting his,her or its personal information and obtain written consent prior to processing personal information. Alternatively, where services or transactions are concluded over the telephone or electronic video feed, EthiQal will maintain a voice recording of the stated purpose for collecting the personal informationfollowed by the data subject's subsequent consent. EthiQal will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected. Where applicable, the data subject must be informed of the possibilitythat their personal information will be shared with other aspects of EthiQal's business and be provided with the reasons for doing so.

Purpose Specification	All of EthiQal's business units and operations must be informed bythe principle of transparency. EthiQal will process personal information only for specific, explicitlydefined and legitimate reasons. EthiQal will inform data subjects of these reasons prior to collectingor recording the data subject's personal information.
Further Processing Limitation	Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose. Therefore, where EthiQal seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, EthiQal will first obtain additional consent from the data subject.
Information Quality	EthiQal will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. The more important it is that the personal information be accurate (for example, the beneficiary details of an insurance policy are of theutmost importance), the greater the effort EthiQal will put into ensuring its accuracy. Where personal information is collected or received from third parties, EthiQal will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with thedata subject or by way of independent sources.
Open Communication	EthiQal will take reasonable steps to ensure that data subjects are notified (are always aware) that their personal information is being collected including the purpose for which it is being collected and processed. EthiQal will ensure that it establishes and maintains a "contact us" facility, for instance via its website or through a monitored emailaddress, for data subjects who want to: • Enquire whether the organisation holds related personal information; or • Request access to related personal information; or • Request the organisation to update or correct related personal information; or Make a complaint concerning the processing of personalinformation.

Security Safeguards	EthiQal will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification ordestruction. Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required. EthiQal will continuously review its security controls which will include regular testing of protocols and measures put in place tocombat cyber-attacks on EthiQal's IT network. EthiQal will ensure that all paper and electronic records comprisingpersonal information are securely stored and made accessible only to authorised individuals. All new employees will be required to sign employment contractscontaining contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which EthiQal is responsible. All existing employees will, after the required consultation process hasbeen followed, be required to sign an addendum to their employmentcontaining the relevant consent and confidentiality clauses. As Set outin **Annexure B** hereto. EthiQal's operators and third-party service providers will be required to enter into service level agreements with EthiQal whereboth parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. Asset out in **Annexure C** hereto.
SPECIFIC DUTIES OF ROLE-PLAYERS	
Governing Body / Board of Directors	EthiQal's governing body cannot delegate its accountability and is ultimately answerable for ensuring that EthiQal meets its legalobligations in terms of POPIA. The governing body may however delegate some of its responsibilitiesin terms of POPIA to management or other capable individuals. The governing body is responsible for ensuring that: • EthiQal appoints an Information Officer, and where necessary, a Deputy Information Officer.

	• All persons responsible for the processing of personal information on behalf of EthiQal are appropriately trained and supervised to do so. • Understand that they are contractually obligated to protect the personal information they come into contact with. • Are aware that a wilful or negligent breach of this policy's processesand procedures may lead to disciplinary action being taken againstthem. • Data subjects who want to make enquires about their personal information are made aware of the procedure that needs to be followed should they wish to do so. • The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which EthiQal collects, holds, uses, shares, discloses, destroys and processes personal information.
Appointment of Information Officer	The appointment of the EthiQal Information Officer will beauthorised by the Chief Executive Officer: • Consideration will be given on an annual basis of the re-appointment or replacement of the Information Officer; and theneed for any Deputy to assist the Information Officer. Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
Information Officer Responsibilities	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 1, and Chapter 5, Part B. The Information Officer is responsible for ensuring compliance with POPIA. The Information Officer has the following responsibilities: • Developing, publishing and maintaining a POPI Policy which addresses all relevant provisions of the POPI Act, including but notlimited to the following: ➢ Reviewing the POPI Act and periodic updates as published. ➢ Ensuring that POPI Act induction training takes place for all staff. ➢ Ensuring that periodic communication awareness on POPIAct responsibilities takes place; and ➢ Ensuring that Privacy Notices for internal and externalpurposes are developed and published. • Handling data subject access requests. • Approving unusual or controversial disclosures of personal data. • Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information. • Ensuring that appropriate Security Safeguards in line with POPI Act for personal information are in place.

	• Handling all aspects of relationship with the Regulator as foreseen in the POPI Act. • Provide direction to any Deputy Information Officer when appointed. • Keeping the governing body updated about EthiQal's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officermust inform and advise the governing body of their obligations pursuant to POPIA. • Continually analysing privacy regulations and aligning them with EthiQal's personal information processing procedures. This will include reviewing EthiQal's information protection procedures and related policies. • Ensuring that POPI Audits are scheduled and conducted on a regular basis. • Ensuring that EthiQal makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to EthiQal. For instance, maintaining a "contact us" facility on EthiQal's website. • Approving any contracts entered with operators, employees andother third parties which may have an impact on the personal information held by EthiQal. This will include overseeing the amendment of EthiQal's employment contracts and other service level agreements. • Encouraging compliance with the conditions required for the lawful processing of personal information. • Ensuring that employees and other persons acting on behalf of EthiQal are fully aware of the risks associated with the processing of personal information and that they remain informed about EthiQal's security controls. • Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of EthiQal. • Addressing employees' POPIA related questions. • Addressing all POPIA related requests and complaints made by EthiQal's data subjects. Working with the Information Regulator in relation to any ongoing investigations. The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consultwith the Information Regulator where appropriate, with regard toany other matter.
IT Manager	EthiQal's IT Manager is responsible for: • Ensuring that EthiQal's IT infrastructure, filing systems and anyother devices used for processing personal information meet acceptable security standards. • Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services. • Ensuring that servers containing personal information are sited in a

	secure location, away from the general office space. • Ensuring that all electronically stored personal information is backed-up and tested on a regular basis. • Ensuring that all back-ups containing personal information are protected from unauthorised access, accidental deletion and malicious shacking attempts. • Ensuring that personal information being transferred electronically is encrypted. • Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software. • Performing regular IT audits to ensure that the security of EthiQal's hardware and software systems are functioning properly. • Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons. • Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on EthiQal's behalf. For instance, cloud • computing services.
Employees and Staff	**Refer to Annexure E**
Processing Limitation	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 2.
Processing Limitation Definition	The act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes: • The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use. • Dissemination by means of transmission, distribution or making available in any other form; or • Merging, linking, as well as any restriction, degradation, erasure or destruction of information. EthiQal undertakes to comply with the POPI Act, Conditions 2 in terms of processing limitation, Sections 9 to 12.
Compliance Control: Formsof consent	EthiQal undertakes to gain written consent where appropriate; alternatively, a recording must be kept of verbal consent.

Identification of PersonalInformation held by EthiQal	EthiQal has engaged in an extensive internal review to identify all instances of personal information held by it and the safeguards in placeto protect such data.
Purpose Specification	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 3.
Purpose specification	EthiQal undertakes to comply with the POPI Act, Conditions 2 in terms of processing limitation, sections 13 and 14, subject to legislated retention periods.
Retention periods	Detailed coverage of the relevant retention periods has been documented in **Annexure D** – Legislation requiring retention of records.
Hard Copies	Paper record archiving takes place using Metrofile, an offsite service provider.
Electronic Storage	The internal procedure requires that electronic storage of information important documents and information must be referred to and discussed with line management who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with thedepartments concerned. 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, except for documents pertaining to personnel.
Further Processing Limitation	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 4.
Further Processing Limitation	EthiQal undertakes to comply with the POPI Act, Conditions 2 interms of processing limitation, Section 15.
Information Quality	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 5. EthiQal will comply with all of the aspects of Condition 5, Section16.

Accuracy	EthiQal will regularly review its procedures for ensuring that itsrecords remain accurate and consistent and, in particular: • ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate data. • Data on any individual will be held in as few places as necessary, and all staff will be discouraged from establishing unnecessary additional data sets. • Effective procedures will be in place so that all relevant systems are updated when information about any individual changes. Staff who keep more detailed information about individuals will begiven additional guidance on accuracy in record keeping
Updating	EthiQal will review all personal information on an annual basis.
Openness	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 6.
Openness	In line with Conditions 6 and 8 of the Act, EthiQal is committed to ensuring that in principle Data Subjects are aware that their data is being processed: • For what purpose it is being processed. • What types of disclosure are likely. • How to exercise their rights in relation to the data.
Procedure	Data Subjects will generally be informed in the following ways: • Staff: through the processes and procedures set out in this policy. • Customers and other interested parties: through the Privacy Notice (Attached hereto as per **Annexure F).** • Whenever data is collected, the number of mandatory fields will bekept to a minimum and Data Subjects will be informed which fields are mandatory and why.
Security Safeguards	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 7, Section 19 to 22. This section of the policy only addresses security issues relating to personal information. It does not cover security of the building, business continuity or any other aspect of security.

Specific Risks	EthiQal has identified the following risks: • Staff with access to personal information could misuse it. • Staff may be tricked into giving away information, either about customers / member or colleagues, especially over the phone or email.
Setting Security Levels	• Access to information on the main EthiQal computer system will be controlled by function. • EthiQal has engaged in an extensive internal due diligenceprocess to identify all instances of personal information held by it and the safeguards in place to protect such data.
Security Measures	EthiQal will ensure that all necessary controls are in place in termsof access to personal information as set out in this policy.
Business Continuity	EthiQal will ensure that adequate steps are taken to providebusiness continuity in the event of an emergency.
Related Policy	Please see the EthiQal Data Governance Framework for further guidance.
Data Subject Participation	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Condition 8, Sections 23 to 25.
Responsibility	Any subject access requests will be handled by the POPI Act Information Officer in terms of Condition 8.
Procedure for Making a Request	Subject access requests must be in writing. All staff are required to passon anything which might be a subject access request to the POPI Act Information Officer without delay. Requests for access to personal information will be handled in compliance with the POPI Act and in compliance with the Promotion of Access to Information Act (PAIA), as defined in the EthiQal PAIA Manual.
Provision for Verifying Identity	Where the individual making a subject access request is not personally known to the POPI Act Information Officer their identity will be verified before handing over any information.
Charging	Fees for access to personal information will be handled in compliancewith the PAIA Act.

Procedure for Granting Access	Procedures for access to personal information will be handled in compliance with the PAIA Act, as defined in the EthiQal PAIA Manual.
Processing of Special Personal Information	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Part B, sections 26 to 33.
Processing of Special Personal Information	EthiQal has the policy of adhering to the process of Special Personal Information which relates to the religious or philosophical beliefs, raceor ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject. Special personal information includes criminal behaviour relating to alleged offences or proceedings dealing with alleged offences. Unless a general authorisation, alternatively a specific authorisation relating to the different types of special personal information applies, a responsible party is prohibited from processing special personal information.
Processing of Personal Information of Children	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Part C, Sections 34 and 35.
Processing of Personal Information of Children	EthiQal has the policy of adhering to the process of Special Personal Information of children. This applies to under-18 individuals, so an agecheck is required for all personal information records. General authorisation concerning personal information of children only applieswhere under-18's are involved. EthiQal has engaged in an extensive internal due diligence process to identify all instances of personal information held by it and the safeguards in place to protect such data and to identify any records held which contain Personal Information of children.
Prior Authorisation	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Chapter 6.
Prior Authorisation	EthiQal has the policy of adhering to the process of PriorAuthorisation in terms of sections 57 to 59.

Direct Marketing, Directories and Automated Decision Making	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Chapter 8.
Direct Marketing, Directories and Automated DecisionMaking	EthiQal undertakes to comply with the POPI Act Chapter 8, Sections 69 to 71. EthiQal through appropriate management of its business partners and counterparty relationships shall hold its partners accountable in respect of any direct marketing undertaken on EthiQal's behalf.
Opting In	Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the Data Subject will be given a clear opportunity to opt in.
Sharing Lists	EthiQal has the policy of sharing lists (or carrying out joint orreciprocal mailings) only on an occasional and tightly controlled basis. Details will only be used for any of these purposes where the Data Subject has been informed of this possibility, along with an option to opt out, and has not exercised this option. EthiQal undertakes to obtain external lists only where it can be guaranteed that the list is up to date and those on the list have been given an opportunity to opt out.
Electronic Contact	Whenever e-mail addresses are collected, any future use for marketingwill be identified, and the provision of the address made optional.
Trans-border Information Flows	
Scope	The scope of this aspect of the policy is defined by the provisions of thePOPI Act, Chapter 9.
Trans-border Information Flows	EthiQal will ensure that the POPI Act Chapter 9, section 72 is fullycomplied with. EthiQal has reviewed its processes to identify Trans border flowswhich contain Personal Information. Compliance with section 72 will be achieved through the use of the necessary contractual commitments from the relevant third parties.

Staff Training and Acceptance of Responsibilities	
Scope	The scope of this aspect of the policy is written in support of the provisions of the POPI Act, Chapter 5, Part B.
Documentation	Information for staff is contained in this policy document and other materials made available by the Information Officer.
Induction	The EthiQal Information Officer will ensure that all staff who have access to any kind of personal information will have their responsibilities outlined during their induction procedures.
Continuing Training	EthiQal will provide opportunities for staff to explore POPI Actissues through training, team meetings, and supervisions.
Procedure for Staff Signifying Acceptance of Policy	EthiQal will ensure that all staff sign acceptance of this policy once they have had a chance to understand the policy and their responsibilities in terms of the policy and the POPI Act.
POPI Complaints Procedure	
Complaints Investigation Procedure	POPI complaints must be submitted to EthiQal in writing. Where sorequired, the Information Officer will provide the data subject with a "POPI Complaint Form". • Where the complaint has been received by any person other thanthe Information Officer, that person will ensure that the full detailsof the complaint reach the Information Officer within 1 working day. • The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within2 working days. • The Information Officer will carefully consider the complaint and address the complainant's concerns in an amicable manner. In considering the complaint, the Information Officer will endeavourto resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA. • The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that hasoccurred and which may have a wider impact on EthiQal's datasubjects. • Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with EthiQal's governing body where after the affecteddata subjects and the Information Regulator will be informed of this breach. • The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to EthiQal's governing body within 7 working days of receipt of the complaint. In all

	instances, EthiQal will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.
	• The Information Officer's response to the data subject may comprise any of the following:
	  • A suggested remedy for the complaint.
	  • A dismissal of the complaint and the reasons as to why it was dismissed; and
	  • An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
	• Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to

	• complain to the Information Regulator. • The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

Disciplinary Action	• Where a POPI complaint or a POPI infringement investigation has been finalised, EthiQal may recommend any appropriate administrative, legal and/or disciplinary action to be taken againstany employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
	• In the case of ignorance or minor negligence, EthiQal will undertake to provide further awareness training to the employee.
	• Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which EthiQal may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
	• Examples of immediate actions that may be taken subsequent to an investigation include:
	  ➢ A recommendation to commence with disciplinary action.
	  ➢ A referral to appropriate law enforcement agencies for criminal investigation.
	  ➢ Recovery of funds and assets in order to limit any prejudice or damages caused.

Policy Review	
Responsibility	The EthiQal Information Officer is responsible for an annual reviewto be completed prior to the policy anniversary date.
Procedure	The EthiQal Information Officer will ensure relevant stakeholders are consulted as part of the annual review to becompleted prior to the policy anniversary date.

ANNEXURE A:
RIGHTS OF DATA SUBJECTS IN TERMS OF POPIA

RIGHTS OF DATA SUBJECTS	
EthiQal's Obligations in so far Rights of Data Subjects and Support thereof	Where appropriate, EthiQal will ensure that its clients andcustomers are made aware of the rights conferred upon them as data subjects. EthiQal will ensure that it gives effect to the following seven rights**:**
The Right to Access Personal Information	1. EthiQal recognises that a data subject has the right to establish whether EthiQal holds personal information related to him, heror it is including the right to request access to that personal information.
The Right to have Personal Information Corrected or Deleted	2. The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where EthiQal is no longer authorised to retain the personal information.
The Right to Object to the Processing of Personal Information	3. The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information. In such circumstances, EthiQal will give due consideration to the request and the requirements of POPIA. EthiQal may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.
The Right to Object to Direct Marketing	4. The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.
The Right to Complain to the Information Regulator	5. The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.
The Right to be Informed	6. The data subject has the right to be notified that his, her or its personal information is being collected by EthiQal. 7. The data subject also has the right to be notified in any situation where EthiQal has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

ANNEXURE B:
EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

1. "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

2. "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

2.1 The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

2.2 The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees that:

2.2.1 he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.

2.2.2 he/she consents and authorises the employer to undertake the collection, processing and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.

2.3 Without derogating from the generality of the aforesaid, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.

2.4 To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.

2.5 To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.

2.6 To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.

2.7 The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day to day basis.

2.8 The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

2.9 The employee acknowledges that during the course of the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers and other employees.

2.10 To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

2.11 Employees may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within EthiQal or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.

ANNEXURE C:
SERVICE LEVEL AGREEMENTS CONFIDENTIALITY UNDERTAKINGS

1. Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person whether the information is recorded electronically or otherwise.

2. "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

3. The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified, or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value.

4. The parties agree that they will at all times comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement.

5. The parties agree that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this agreement.

6. Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.

ANNEXURE D:
RETENTION PERIODS IN TERMS OF PREVAILING APPLICABLE LEGISLATION

Retention periods	
Companies Act, No 71 of 2008	With regard to the Companies Act, No 71 of 2008 and the Companies Amendment Act No 3 of 2011, hard copies of the documents mentioned below must be retained for 7 years: • Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act. • Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities. • Copies of reports presented at the annual general meeting of the company. • Copies of annual financial statements required by the Act. • Copies of accounting records as required by the Act. • Record of directors and past directors, after the director has retired from the company. • Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' Committees. • Copies of the documents mentioned below must be retained indefinitely: ➢ Registration certificate. ➢ Memorandum of Incorporation and alterations and amendments. ➢ Rules. ➢ Securities register and uncertified securities register. ➢ Register of company secretary and auditors; and ➢ Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register ofdisclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

Consumer Protection Act, No 68 of 2008:	The Consumer Protection Act seeks to promote a fair, accessible and sustainable marketplace and therefore requires a retention period of 3 years for information provided to a consumer by an intermediary such as: • Full names, physical address, postal address and contact details. • ID number and registration number. • Contact details of public officer in case of a juristic person. • Service rendered. • Intermediary fee. • Cost to be recovered from the consumer. • Frequency of accounting to the consumer. • Amounts, sums, values, charges, fees, remuneration specified in monetary terms. • Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided. • Record of advice furnished to the consumer reflecting the basis on which the advice was given. • Written instruction sent by the intermediary to the consumer. • Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions. • Documents Section 45 and Regulation 31 for Auctions.

Financial Advisory and Intermediary Services Act,No 37 of 2002	Section 18 of the Act requires a retention period of 5 years, except to the extent that it is exempted by the registrar for the below mentioned documents:
	
	• Known premature cancellations of transactions or financial products of the provider by clients.
	• Complaints received together with an indication whether or not any such complaint has been resolved.
	• The continued compliance with this Act and the reasons for such non-compliance.
	• The continued compliance by representatives with the requirements referred to in section 13(1) and (2).
	• The General Code of Conduct for Authorized Financial Services Provider.
	• Representatives requires a retention period of 5 years for the below mentioned documents:
	  • Proper procedures to record verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of Section 15 of the Act;
	  • Store and retrieve such records and any other material documentation relating to the client or financial services

	rendered to the client. • And keep such client records and documentation safe from destruction. • All such records must be kept for a period after terminationto the knowledge of the provider of the product concernedor in any other case after the rendering of the financial service concerned.
Financial Intelligence Centre Act, No 38 of 2001	Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below: • Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client. • If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the client's authority to act on behalf of that other person. • If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client. • The manner in which the identity of the persons referred to above was established. • The nature of that business relationship or transaction. • In the case of a transaction, the amount involved and the parties to that transaction. • All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction. • The name of the person who obtained the identity of the person transacting on behalf of the accountable institution. • Any document or copy of a document obtained by the accountable institution. • These documents may also be kept in electronic format.

Compensation for Occupational Injuries and Diseases Act, No 130 of 1993	Section 81(1) and (2) of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below: ▯ Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees. ▯ POPI Policy 11− Section 20(2) documents with a required retention period of 3 years: ➢ 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; and ➢ Records of incidents reported at work. ▯ Asbestos Regulations, 2001, Regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below: ➢ Records of assessment and air monitoring, and the asbestos inventory; and ➢ Medical surveillance records. Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): ➢ Records of risk assessments and air monitoring; and ➢ Medical surveillance records. • Lead Regulations, 2001, Regulation 10: ➢ Records of assessments and air monitoring; and ➢ Medical surveillance records. • Noise - induced Hearing Loss Regulations, 2003, Regulation 11: ➢ All records of assessment and noise monitoring; and ➢ All medical surveillance records, including the baseline audiogram of every employee. • Hazardous Chemical Substance Regulations, 1995, Regulation 9 requires a retention period of 30 years for the documents mentioned below: ➢ Records of assessments and air monitoring; and Medical surveillance records.

Basic Conditions of Employment Act, No 75 of 1997	The Basic Conditions of Employment Act requires a retention period of 3 years for the documents mentioned below:
	
	• Section 29(4):
	  ➢ Written particulars of an employee after termination of employment.
	• Section 31:
	  ➢ Employee's name and occupation.
	  ➢ Time worked by each employee.
	  ➢ Remuneration paid to each employee.
	  ➢ Date of birth of any employee under the age of 18 years.

Employment Equity Act, No 55 of 1998	Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 years for the documents mentioned below: • Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act. • Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.

Labour Relations Act, No 66 of 1995	Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:
	
	• The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings.
	• Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings.
	• Registered Trade Unions and employer's organizations must retain the ballot papers.
	• Records to be retained by the employer are the collective agreements and arbitration awards.
	• Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:
	  ➢ Registered Trade Unions and registered employer's organizations must retain a list of its members.
	  ➢ An employer must retain prescribed details of any strike action involving its employees.

	➢ Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions. The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.
Unemployment Insurance Act, No 63 of 2002	The Unemployment Insurance Act, applies to all employees and employers except: • Workers working less than 24 hours per month. • Learners. • POPI Policy 13. • Public servants. • Foreigners working on a contract basis. • Workers who get a monthly State (old age) pension. • Workers who only earn commission. • Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the documents mentioned below: ➢ 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.
Tax Administration Act, No 28 of 2011	Section 29 of the Tax Administration Act, states that records of documents must be retained to: • Enable a person to observe the requirements of the Act. • Are specifically required under a Tax Act by the Commissioner by the public notice. • Will enable SARS to be satisfied that the person has observed these requirements. Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until the return is submitted, then a 5 year period applies for taxpayers who were meant to submit a return. • Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption. • Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the

	assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.
Income Tax Act, No 58 of 1962	Schedule 4, paragraph 14(1)(a)-(d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep: • Amount of remuneration paid or due by him to the employee. • The amount of employee's tax deducted or withheld from theremuneration paid or due. • The income tax reference number of that employee; (POPI Policy 14). • Any further prescribed information. • Employer Reconciliation return. Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to: • Amounts received by that registered micro business during a year of assessment. • Dividends declared by that registered micro business during a year of assessment. • Each asset as at the end of a year of assessment with cost price of more than R 10 000. • Each liability as at the end of a year of assessment that exceeded R10 000.

Value Added Tax Act, No 89 of 1991	Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 years from the date of submission of the return for the documents mentioned below: • 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. • 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. • 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. • Documentary proof substantiating the zero rating of supplies. • 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.

ANNEXURE E
SPECIFIC DUTIES OF EMPLOYEES

1. Employees and other persons acting on behalf of EthiQal will, during the performance of their duties gain access to and become acquainted with the personal information of policyholders, suppliers and other employees.

2. Employees and other persons acting on behalf of EthiQal are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

3. Employees and other persons acting on behalf of EthiQal may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party, either within EthiQal or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties.

4. Employees and other persons acting on behalf of EthiQal must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

5. Employees and other persons acting on behalf of EthiQal will only process personal information where:

    5.1 The data subject, or a competent person where the data subject is a child, consents to the processing; or

    5.2 The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or

    5.3 The processing complies with an obligation imposed by law on the responsible party; or

    5.4 The processing protects a legitimate interest of the data subject; or

    5.5 The processing is necessary for pursuing the legitimate interests of EthiQal or of a third party to whom the information is supplied.

6. Furthermore, personal information will only be processed where the data subject:

    6.1 Clearly understands why and for what purpose his, her or its personal information is being collected; and

    6.2 Has granted EthiQal with explicit written or verbally recorded consent to process his,her or its personal information.

7. Employees and other persons acting on behalf of EthiQal will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
8. Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with.

9. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form.
10. Alternatively, EthiQal will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
11. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

    11.1 The personal information has been made public, or

    11.2 Where valid consent has been given to a third party, or

    11.3 The information is necessary for effective law enforcement.

12. Employees and other persons acting on behalf of EthiQal will under no circumstances:

    12.1 Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.

    12.2 Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from EthiQal's central database or a dedicated server.

    12.3 Share personal information informally.

    12.4 Personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.

    12.5 Transfer personal information outside of South Africa without the express permission from the Information Officer.

13. Employees and other persons acting on behalf of EthiQal are responsible for:

    13.1 Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
    13.2 Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
    13.3 Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of EthiQal, with the sending or sharing of personal information to or with authorised external persons.

    13.4 Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
    13.5 Ensuring that their computer screens and other devices are switched off or locked when

not in use or when away from their desks.

13.6 Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.

13.7 Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.

13.8 Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.

13.9 Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.

13.10 Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.

13.11 Undergoing POPI Awareness training from time to time.

14. Where an employee, or a person acting on behalf of EthiQal, becomes aware or suspicious ofany security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

ANNEXURE F:
ETHIQAL CUSTOMER PRIVACY NOTICE

EthiQal respects the right to privacy and confidentiality of our potential and existing client's personal information. We are committed to protecting your privacy and to ensure that your personal information is collected and used properly, lawfully and transparently. This notice extends to all entities within EthiQal, as noted above.

1. This privacy notice is meant to help you understand how we collect, use, share and protect your personal information. EthiQal subscribes to the conditions of the Protection of Personal Information Act (POPIA) as well as the principles set out in Section 51 of the Electronic Communications and Transactions Act 25 of 2002 to make sure that you are always protected when supplying us with personal information.

2. We subscribe to the principles, outlined in Section 51 of the ECT Act and POPI Act, which govern your right to having your personal information kept private. We briefly outline these principles below:

    3.1 We shall only collect, collate, process and store ('use') your personal information with your written permission as set out in this policy, unless legally required to do so, and will only use such information for the lawful purpose for which it is required as set out in this policy.

    3.2 We shall disclose in writing, upon request, the specific purpose for which we use, collect and store your personal information. We will also keep a record of that personal information and the specific purpose for which we have used it.

    3.3 We will not use your personal information for any purpose, other than that which we disclosed to you herein, unless you give us your express written permission to do so, or unless we are permitted/required to do so, by law.

3. The Protection of Personal Information Act 9 (POPIA) describes personal information as information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person.

4. The person to whom personal information relates is referred to as the "data subject".

5. <u>What type of personal information do we collect?</u>

The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose. When personal information is collected, the company will indicate the purpose for the collection and whether the information required is compulsory or voluntary.

Examples of personal information include, but are not limited to, contact information, financial information, information relating to race, gender, sexual orientation, age, contact details, identity number, religion, name, culture, language and nationality.

6. How we collect personal information?

The company collects information either directly from the data subject, the employer or through intermediaries. The source from which personal information was obtained, if not directly from the data subject, will be disclosed.

7. Use of personal information

After obtaining consent, the personal information collected or held by EthiQal may be used, stored, transferred or disclosed or shared only for the purposes for which it was collected or agreed with you. This may include:

8.1 For underwriting purposes.

8.2 To assess and process claims.

8.3 Providing on-going administration services for the duration of the contract (policy of insurance).

8.4 Fulfilling a transaction on request of a data subject.

8.5 To respond to your inquiries and/or complaints.

8.6 To confirm and verify your identity or to verify that you are an authorised person for security purposes.

8.7 For the detection and prevention of fraud, crime, money laundering or other malpractice.

8.8 Providing you with products or services and complying with your instructions.

8.9 Assisting in improving Group entities' services, and providing you with information via mail, telephone or other means about Group entities services. Note that, as permitted by the ECT Act, this website may use personal information collected to compile profiles for statistical purposes and trade in these profiles. No information contained in the profiles or statistics will be able to be linked to any specific user.

8.10 Group entities may share your personal information with third parties for purposes of management and administration of this Website.

8.11 Records of personal information will be retained for the period necessary for achieving the purpose for which the information was collected. Please note that you have a right to object to the processing of your personal information for example for purposes of direct marketing, unless consent was obtained from you.

8. Methods of processing

Data processing is carried out using computers and/or IT-enabled tools, following organisational procedures and modes strictly related to the purposes indicated. In some cases, the data may be

accessible to certain types of persons in charge, involved with the operations inside EthiQal (underwriting, compliance, marketing, legal, system administration, etc.) or external parties (such as third-party technical service providers, mail carriers, hosting providers, IT companies, communications agencies) appointed, if necessary, as data processors by EthiQal.

9. Our website

10.1 We take reasonable and necessary precautions to secure your transactions on our website - however, we cannot guarantee the confidentiality of your transactions.

10.2 Using our website is entirely at your own risk.

10.3 EthiQal will not be held legally responsible for any personal information that you revealto a third party, which has a link on the www.EthiQal.co.za website. It is important thatyou refer to that third party's privacy notice before you reveal any of your personal information.

10.4 In addition to the personal information you submit, we may collect information about your computer including, where available, your IP address, operating system and browser type for system administration.

10.5 We collect aggregated site-visitation statistics using cookies. We do not track individuals' use of the site. When someone visits the site, a cookie is placed on the customer's machine (if the customer accepts cookies) or is read if the customer has visited the site previously.

10. Cookies and usage data

11.1 Place of processing: South Africa.

11.2 A cookie is a small text file stored on your device by the website you are visiting.

11.3 The EthiQal website may make use of cookie and tracking technology, where information that you send while on the website, is saved on your hard drive. This allows the EthiQal website to recognise you on your next visit. This technology is useful for gathering information, such as the type of browser and operating system you use.

11.4 The information will enable us to track the number of visitors to our website and understand how visitors use it. Personal information cannot be collected via cookie technology.

11.5 You can limit the collection of your information by disabling cookies on your browser. You may also be able to modify your browser settings to require your permission each time a site attempts to set a cookie. However, EthiQal relies on cookies to enable certain functionality. If you choose to disable cookies, you will still have access to the website and its functions, but some of the services available on our website may not work properly.

11.6 This privacy notice may be amended from time to time without any notice to you. Every time you use our website, you are automatically bound to the privacy notice that is current at that moment.

11.7 EthiQal uses SSL Web Server Certificates to offer secure communications. At each point where information is captured the secure padlock symbol will appear in your browser showing that all communication is encrypted.

11. Analytics

12.1 Services contained in this section enable EthiQal to monitor and analyse web traffic andcan be used to keep track of user behaviour.

12.2 Google Analytics may be used. These are web analysis service providers that utilize the data collected to track and examine the use of the EthiQal website, to prepare reportson its activities to improve the site's user experience and performance.

12.3 Each web service provider is responsible for adherence to relevant data protection rules which can be obtained via their own Privacy Notice.

12. Disclaimer

13.1 Apart from the provisions of sections 43(5) and 43(6) of the Electronic Communications and Transactions Act, as amended, EthiQal nor any of its agents or representatives shallbe liable for any damage, loss or liability of whatsoever nature arising from the use or inability to use this web site or the services or content provided from and through this website. Furthermore, EthiQal makes no representations or warranties, implied or otherwise, that, amongst others, the content and technology available from this website are free from errors or omissions or that the service will be 100% uninterrupted and errorfree. Users are encouraged to report any possible malfunctions and errors to the webmaster.

13.2 Information, ideas and opinions expressed on this site should not be regarded as professional advice of EthiQal, but users are encouraged to consult professional advice before taking any course of action related to information, ideas or opinions expressed on this site.

13.3 Neither EthiQal nor any of its agents or representatives shall be liable for any damage,loss or liability of whatsoever nature arising from the use or inability to use this web site orthe information on this web site.

13. Sharing of personal information

EthiQal will only share your personal information with third parties if you have consented to such disclosure. If consent has been obtained, EthiQal may share your personal information with third parties who are involved in the delivery of services to you.

We have agreements in place to ensure that they comply with the Protection of Personal Information Act, No 4 of 2013.

Where EthiQal discloses personal information to any third parties, the third party will be obliged to use that personal information only for the reasons and purposes it was disclosed for. All service

providers are bound by contract to maintain the confidentiality and security of your personal information and are restricted in their use thereof as per this policy.

We may be obliged to disclose your personal information to the extent that it is required to do so by law, in connection with any legal proceedings or prospective legal proceedings, or for the purposes of protecting the interest of clients, for example fraud prevention or to give effect to an agreement.

14. Securing personal information

EthiQal processes the data of data subjects in a proper manner and shall take appropriate security measures to prevent loss or damage of personal information, unauthorised access, disclosure, modification, or unauthorised destruction of the data.

EthiQal stores all the personal information in secured environments, for example on secured servers in a protected data centre.

15. Right to access and rectify personal information collected

You have the right to request to review your personal information contained by EthiQal at anytime to correct or update the information.

If the purpose for which your personal information was requested initially does not exist anymore, for example you no longer have an active contract, you may request information held by the company to be removed. However, EthiQal can decline your request to delete the information from its records if legislation requires the continued retention thereof or if it has been de-identified.

If you would like to obtain a copy of your personal information held by EthiQal, please reviewour information manual.

16. Right to lodge a Complaint to the Information Regulator

Any person may submit a complaint to the Regulator alleging interference with the protection of the personal information of a data subject.

17. Updating this Notice

Please note that we may amend this Notice from time to time. Please check this website periodically to inform yourself of any changes.

18. How to Contact us

This Privacy Notice applies to EthiQal, incorporating all its operating entities.

Please direct any questions, complaints or concerns regarding this privacy notice, data privacy and our treatment of your Personal Information to the following:

Upon receiving your request, we will contact you directly, investigate your request, and work to address your concerns. We will respond to your request without undue delay. We reserve the right to take reasonable steps to verify your identity prior to granting access or processing changes or corrections.

19. INFORMATION REGULATOR

You have the right to complain to the Information Regulator, whose contact details are:
Tel: 012 406 4818
Fax: 086 500 3351

Email: inforeg@justice.gov.za