Technologies KZN

A:
PROTECTION OF PERSONAL INFORMATION IN TERMS OF THE POPIA

1.1 COMPANY ASSURANCE

Thyme Technologies KZN is a company functioning within the IT, Finance and Payroll business and is committed to comply with The Protection of Personal Information Act 4 of 2013.

POPI requires Thyme Technologies KZN to inform their clients as to the way their personal information is used, disclosed, and destroyed.

Thyme Technologies KZN guarantees its commitment to protecting its client's privacy and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

The Policy sets out the way Thyme Technologies KZN deals with their client's personal information and stipulates the purpose for which said information is used. The Policy is made available on the company website www.thyme.co.za.

1.2 PERSONAL INFORMATION COLLECTED

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

Thyme Technologies KZN collects and processes client's personal information pertaining to the client's requirements. The type of information will depend on the requirements for which it is collected and will be processed for that purpose only.

Whenever possible, Thyme Technologies KZN will inform the client as to the information required and the information deemed optional. Examples of personal information we collect include, but is not limited to:

- The Client's Identity number, name, surname, address, postal code, marital status, and number of dependents.

- Description of the client's residence, business, assets; financial information, banking details, etc.-.

Thyme Technologies KZN also collects and processes the client's personal information for marketing purposes to ensure that our products and services remain relevant to our clients and potential clients.

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

With the client's consent, Thyme Technologies KZN may also supplement the information provided with information Thyme Technologies KZN receives from other providers in order to offer a more consistent and personalized experience in the client's interaction with Thyme Technologies KZN.

For purposes of this Policy, clients include potential and existing clients.

1.3 THE USAGE OF PERSONAL INFORMATION

The Client's Personal Information will only be used for the purpose for which it was collected and as agreed. This may include:

• Providing products or services to clients and to carry out the transactions requested.
• Conducting credit reference searches or- verification.
• Confirming, verifying, and updating client details.
• Conducting market or customer satisfaction research.
• For audit and record keeping purposes.
• In connection with legal proceedings.
• Providing Thyme Technologies KZN services to clients, to render the services requested and to maintain and constantly improve the relationship.
• Providing communication in respect of The Thyme Technologies KZN and regulatory matters that may affect clients; and
• In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

According to section 10 of POPI, personal information may only be processed if certain conditions, listed below, are met along with supporting information for Thyme Technologies KZN processing of Personal Information:

a) The client's consents to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship.

b) The necessity of processing: to conduct an accurate analysis of the client's needs for purposes of amongst other credit limits.

c) Processing complies with an obligation imposed by law on the Thyme Technologies KZN.

d) Processing protects a legitimate interest of the client — it is in the client's best interest to have a full and proper needs analysis performed to provide them with an applicable and beneficial product or service.

e) Processing is necessary for pursuing the legitimate interests of the Thyme Technologies KZN or of a third party to whom information is supplied — in order to provide Thyme Technologies KZN clients with products and or services both Thyme Technologies KZN and any of our product suppliers require certain personal information from the clients in order to make an expert decision on the unique and specific product and or service required.

1.4 DISCLOSURE OF PERSONAL INFORMATION

Thyme Technologies KZN may disclose a client's personal information to any of the Thyme Technologies group of companies, or approved product or third-party service providers whose services or products clients elect to use.

Thyme Technologies KZN has agreements in place to ensure that compliance with confidentiality and privacy conditions.

Thyme Technologies KZN may also share client personal information with and obtain information about clients from third parties for the reasons already discussed above.

Thyme Technologies KZN 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 Thyme Technologies KZN rights.

1.5 SAFEGUARDING CLIENT INFORMATION

It is a requirement of POPI to adequately protect personal information. Thyme Technologies KZN will continuously review its security controls and processes to ensure that personal information is secure.

The following procedures are in place to protect personal information:

1.5.1 THE Thyme Technologies KZN Information Officer is Julie Ramseier whose details are available below and who is responsible for the compliance with the conditions of the lawful processing of personal information and other provisions of POPI.

POSTAL ADDRESS: PO Box 91, Bothas Hill, 3610
PHYSICAL ADDRESS: Lot 181, 5 Nyala Drive, Drummond, 3626
E-MAIL ADDRESS: julie@thymetech.co.za
WEBSITE: www.Thyme Technologies.co.za

2. AMENDMENTS TO THIS POLICY

Amendments to, or a review of this Policy, will take place on an *ad hoc* basis or at least once a year. Clients are advised to access Thyme Technologies website periodically to keep abreast of any changes. Where material changes take place, clients will be notified directly, or changes will be stipulated on the Thyme Technologies website.

B:
POLICY ON THE RETENTION & CONFIDENTIALITY OF DOCUMENTS, INFORMATION AND ELECTRONIC TRANSACTIONS

1. **PURPOSE**

1.1 To exercise effective control over the retention of documents and electronic transactions:

1.1.1 as prescribed by legislation; and

1.1.2 as dictated by business practice.

1.2 Documents need to be retained to prove the existence of facts and to exercise rights the Company may have. Documents are also necessary for defending legal action, for establishing what was said or done in relation to business of the Company and to minimize the Company's reputational risks.

1.3 To ensure that the Company's interests are protected and that the Company's and clients' rights to privacy and confidentiality are not breached.

2. **SCOPE & DEFINITIONS**

2.1 All documents and electronic transactions generated within and/or received by the Company.

2.2 Definitions:

2.2.1 **Clients** includes, but are not limited to, debtors, creditors as well as the affected personnel and/or departments related to a service division of the Company.

2.2.2 **Confidential Information** refers to all information or data disclosed to or obtained by the Company by any means whatsoever and shall include, but not be limited to:

2.2.1 **Financial information and records**; and

2.2.2 all other information including information relating to the structure, operations, processes, intentions, product information, know-how, trade secrets, market opportunities, customers and business affairs but excluding the exceptions listed in clause 3.1 hereunder.

2.2.3 **Constitution**: Constitution of the Republic of South Africa Act, 108 of 1996.

2.2.4 **Data** refers to electronic representations of information in any form.

2.2.5 **Documents** include books, records, security or accounts and any information that has been stored or recorded electronically, photographically, magnetically, mechanically, electro-mechanically or optically, or in any other form.

2.2.6 **Electronic communication** refers to a communication by means of data messages.

2.2.7 **Electronic signature** refers to data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

2.2.8 **Electronic transactions** include e-mails sent and received.

3. **ACCESS TO DOCUMENTS**

3.1 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 (also see clause 3.2 below):

3.1.1 where disclosure is under compulsion of law.

3.1.2 where there is a duty to the public to disclose.

3.1.3 where the interests of the Company require disclosure; and

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

3.2 Disclosure to 3rd parties: All employees have a duty of confidentiality in relation to the Company and clients. In addition to the provisions of clause 4.1 above, the following are also applicable:

3.2.1 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of ECTA (Electronic Consumer Transaction Act). Information may be given to a 3rd party if the client has consented in writing to that person receiving the information.

3.2.2 Requests for company information.

3.2.2.1 These are dealt with in terms of PAIA (Promotion of access to information Act), 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 Company, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

3.2.2.2 In terms hereof, requests must be made in writing on the prescribed form to the Company Secretary, who is also 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.

3.2.3 Confidential company and/or business information may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Company must be always kept strictly confidential.

3.3 The Company 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.

4. STORAGE OF DOCUMENTS

4.1 **Hard Copies**

4.1.1 Documents are stored in a different location.

4.1.2 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, hardcopies 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.

Copies of the documents mentioned below must be retained indefinitely:
- Registration certificate.
- Memorandum of Incorporation and alterations and amendments.
- Rules.
- Register of company representative

4.1.3 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.

4.1.4 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 5 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. Section 20(2) documents with a required retention period of 5 years:
- Records of incidents reported at work.

4.1.5 Basic Conditions of Employment Act, No 75 of 1997:

The Basic Conditions of Employment Act requires a retention period of 5 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.

4.1.6 Employment Equity Act, No 55 of 1998:

Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 5 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 5 years for the report which is sent to the Director General as indicated in the Act.

4.1.7 Labour Relations Act, No 66 of 1995:

4.1.8 Sections 53(4), 98(4) and 99 require a retention period of 5 years for the documents mentioned below:

- 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:

- An employer must retain prescribed details of any strike, lock-out or protest 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.

4.1.9 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.
- 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.

4.1.10 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 but have not.

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.

4.1.11 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 the remuneration paid or due.
- The income tax reference number of that employee.
- Any further prescribed information.
- Employer Reconciliation return.

4.1.12 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.

4.2 ELECTRONIC STORAGE

4.2.1 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 and companies concerned.

4.2.2 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. 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 5 years after termination of employment.

4.2.3 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.

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

5. DESTRUCTION OF DOCUMENTS

5.1 Documents may be destroyed after the termination of the retention period specified in Annexure "A" hereto. Registration will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

5.2 Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked 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 Company pending such return.

5.3 After completion of the process in 5.2 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 Registration.

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

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

J Ramseier
Information Officer
01/06/2021

R Ramseier
Director
01/06/2021