

**Legoux Pty Ltd.**

**THE PROTECTION OF PERSONAL INFORMATION ACT  
(ACT 4 OF 2013)**

**POLICY**

**POPIA POLICY FOR Legoux Pty Ltd .**

## **1. INTRODUCTION**

POPIA places certain limitations to the right to access personal information which should be subject to justifiable limitations, which includes the limitations aimed at reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance.

In terms of POPIA we are required to inform the consumer/client as to the manner in which their personal information is processed and to do so in a manner that is appropriate, transparent, secure and in accordance with law.

This Policy will be made available on our website [www.legouxsa.com](http://www.legouxsa.com) and can be requested at our offices.

## **2. PURPOSE OF THE POLICY**

The purpose of this policy is to inform our clients and employees (herein after referred to as data subjects) of the measures we have in place to comply with the laws in respect of personal information we hold for our data subjects.

Legoux Pty Ltd. will follow good practice to prevent a data breach and safeguard our data subject's information against loss or breach of their personal information.

## **3. BACKGROUND**

The purpose of POPIA is to regulate the processing of personal information of data subjects by public and private bodies.

## **4. DEFINITIONS**

(a) Data Subject means the person to whom personal information relates;

(b) POPIA – Protection of Personal Information Act (Act 4 of 2013);

(c) Processing relates to everything you can do with personal information - this includes: collecting, storing, viewing, printing, displaying, archiving, sharing, changing, merging, organising, updating, modifying, deleting and sending the information by way of fax, e-mail, sms etc.

(d) Record, means any recorded information regardless of what form or medium and includes any of following:

- Writing of any material;
- Information produced, recorded, stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any other material subsequently derived from information so produced, recorded or stored.
- Book, map, plan, graph, drawing, label, photograph, film, negative, tape etc.
- That is in the possession or control of a responsible party whether or not it was created by the responsible party and regardless of how it came into existence.

(e) Responsible party means a public or a private body or any other person which, alone or in conjunction with others determines the purpose of and means of processing personal information.

(f) Personal Information means information about a data subjects identifiable, living, natural person and where it is applicable a juristic person including but not limited to:

- Information relating to gender, race, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, wellbeing, disability, religion, conscience, belief, culture, language, and birth of the person.
- Information relating to a person's education, medical, financial, criminal or employment history;
- Identification number, e-mail address, physical address, contact details, location;
- Biometric information;
- Personal opinions or views of the person;

## 5. RESPONSIBILITIES

Legoux Pty Ltd. guarantees its commitment to protecting our client's privacy and ensuring their personal information is used appropriately, transparently, securely and in accordance with applicable laws, as far as it applies to our services.

## 6. CONDITIONS FOR LAWFULL PROCESSING

(a) **Accountability:** The Responsible party must ensure that all conditions as set out in POPIA are complied with at all times. The Responsible party will try and prevent data breaches and safeguard the data subject's personal information by accepting the value of the information it holds.

(b) Processing Limitations:

- The Data Subject must consent to the processing of their personal information;
- The information collected must be used for the purpose it was collected for. Before further processing of the personal information, the responsible party must make sure that the processing is compatible and must take the following into account:
  - The relationship between the purpose of the intended further processing and the purpose for which the information was initially collected;
  - The nature of the information concerned and what consequences there will be for the data subject;
  - The manner in which the information has been collected and if there are any contractual rights and obligations between the parties.
- If we need to process information any further than it was acquired for, we will inform the data subject and get his/her consent to do so.
- Personal Information must be collected from the data subject;
- The data subject needs to consent to the use of their personal information;
- The data subject must understand for which purpose the information will be processed;

- The data subject may object at any time, or ask for the deletion of their personal information.

(c) Specific Purpose:

- The collection of personal information must be collected for a specific purpose that is related to the function or activity of the responsible party.
- The data subject must be aware of the purpose for collection of their personal information and must consent thereto.
- The records must not be retained for longer than necessary, except if the retention is required by law.
- If retention is not necessary all personal information must be destroyed or deleted and it must be done in such a manner that prevents its reconstruction in an intelligible form.
- The information officer will ensure that the information collected will not be used for any other purpose before obtaining the consent of the data subject;
- The information officer will ensure that the person collecting the information will be able to explain to the data subject why this information needs to be collected. The data collected will be limited, we will be able to disclose it to the data subject on request and make sure that retention principles are respected in identifying why personal information is collected.

(d) Limiting collection and further processing:

- The data collected must be in accordance and/or compatible with the purpose for which it is/was collected.
- The responsible party shall ensure that personal information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the personal information was collected for.

(e) Information quality:

- Information collected must be complete, accurate, not misleading and updated on the request of the data subject or where necessary.

(f) Openness

Legoux Pty Ltd. must take reasonable steps to ensure that the data subject is aware of:

- The information being collected;
- The name and address of the responsible party;
- The purpose for which the information has been collected;
- Whether or not the supply of information is voluntarily or mandatory;
- The consequences of failure to provide the information;
- Any law authorising the collection of data;
- The right to access and rectify the information;
- If the responsible party's intention is to provide the information to a third party;
- The right to object to the processing of the information;
- Please see Annexure "A" attached hereto. This sets out the information collected by each department and how we process personal information of our data subject's to enable us to complete the service/purpose appointed for. Kindly note that one department might request documents from another department to be able to complete the service/purpose appointed for.

(g) Security Safeguards;

- The responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical organisational measures.
- All information of data subjects must be treated as confidential and not to be disclosed unless it is required by law;
- The processing must be governed by a written contract/mandate ensuring that safeguards are in place and if domiciled outside of South Africa comply with local protection of personal information laws.

- The data subject may request the responsible party to correct or delete the personal information if it is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
- The data subject may request the information officer to delete or destroy personal information that the responsible party is no longer authorised to obtain. The information officer shall ensure that all employees knows the importance of keeping personal information confidential and shall make sure that when the information is disposed or destroyed, it is done in a manner that will prevent unauthorised parties from gaining access thereto.
- The responsible party shall notify the Information Regulator and the data subject if there is any breach.
- Breach can include but is not limited to, a hacker hacking any computer, files stolen from the office or when a mobile device, tablet or USB goes missing or is stolen with personal information of data subjects on the device.
- A breach can also occur when one of your employees relocates and copies some of the data stored the server.
- Employees will be made aware by the Information Officer of the seriousness of a breach and will report any of the activities that can lead to a breach as mentioned above immediately to the Information Officer.

## **7. INFORMATION REGULATOR**

The Information Regulator has jurisdiction throughout South Africa, they are independent and subject to the Constitution and must exercise its powers and perform its functions in accordance with PAIA and are accountable to the National Assembly. They can enforce penalties and offences, minor offences can be fined and/or imprisonment up to 12 months and major offences by the Regulator can be fined and/or imprisonment for up to 10 years.

## **8. INFORMATION OFFICER RESPONSIBILITIES**

The core focus or duties under POPIA for the Information Officer will be the following:

- (a) Encourage compliance with the information protection conditions as set out in terms of Section 55 of POPIA;
- (b) Developing, publishing and maintaining a POPIA Policy which addresses all relevant provisions of POPIA;
- (c) Reviewing POPIA and periodic updates as published;
- (d) Ensuring POPIA induction training takes place for all staff;
- (e) Ensuring that periodic communication awareness on POPIA responsibilities takes place;
- (f) Ensuring that privacy Notices for internal and external purposes are developed and published;
- (g) Handling data subject access requests;
- (h) Approving unusual or controversial disclosures of personal data;
- (i) Approving contact with Data Operators;
- (j) Ensuring that appropriate policies and controls are in place for ensuring the Information Quality of personal information;
- (k) Ensuring that appropriate Security Safeguards in line with POPIA for personal information are in place;
- (l) Consider requests made pursuant to POPIA;
- (m) Work with the Regulator in relation to investigation conducted pursuant to Chapter 6 against Legoux Pty Ltd.
- (n) Identify and govern all privacy related risks;
- (o) Map all activities performed concerning the collection and storage of personal information i.e. before and post POPIA;
- (p) Know, understand and ensure corporate compliance with all relevant laws of foreign jurisdictions in which we conduct business;
- (q) Coordinate the development, implementation and maintenance of corporate customer and employee privacy policies;
- (r) Ensure compliance with corporate privacy policies and procedures throughout the body.
- (s) Liaise with Human Resources and Legal Departments to ensure standards of disciplinary action and sanction for non-compliance. Liaise with Public Relations and Marketing Departments to create public information communications and procedures on privacy efforts, related issues and breaches.

- (t) Create standards or scripts for responding to clients or public enquiries.
- (u) Create and implement procedures and standards to facilitate customer verification of captured and stored personal information files;
- (v) Monitor and control the privacy requirements and responsibilities of information processing service providers or operators in terms of section 20 and 21 of POPIA.
- (w) Manage breach and incident investigation processes;
- (x) Create and implement our breach management plan, privacy alerts and other privacy related operational issues and to create standards and procedures to manage any compromise in the security of the stored personal information correctly and appropriately. This will include but is not limited to a policy signed by all employees setting out the importance of good practice with their devices and to make sure that the building is secure and that there is no access of files to any third party.
- (y) Investigate, analyse and document all privacy related incidents and complaints.
- (z) Apply investigation findings to update standards, processes and systems as an on-going operational improvement routine.

## **9. TRANSBORDER INFORMATION FLOW**

This is dealt with in terms of Chapter 9, Section 72 of POPIA and Legoux Pty Ltd. will take all reasonable steps to comply herewith and to make sure that we have consent from the data subject before personal information will be transferred overseas.

The transfer of personal information needs to be necessary for the conclusion of the agreement between the responsible party and the data subject and will be to the benefit of the data subject.

Compliance with this section will be achieved through the use of the necessary contractual commitments from the relevant third parties.

## **10. SAFEGAURDING PERSONAL INFORMATION**

It is a requirement of POPIA that we adequately protect the Personal Information we hold and to take all reasonable steps to avoid unauthorized access and use of our client's personal information. We continuously review our security controls and processes to ensure that our client's personal information are secured.

The following procedures are in place to protect our data subject's personal information:

- (a) We run a domain environment where access to data is controlled by user rights and passwords, therefore to access company data on our network you will need to be an authenticated user with the correct rights.
- (b) The network is protected by dual firewalls blocking intrusions from outside.
- (c) The emails are running on Office 2016 exchange systems and they are protected by Microsoft's systems for e-mail transfers.
- (d) Devices that travel offsite are protected by built in encryption, usernames and passwords.
- (e) Legoux Pty Ltd uses SAGE ONE accounting services. SAGE ONE POPIA policy may be requested if required.
- (f) We have appointed R Gouws as the information officer and T Gouws as the deputy information officer, whose details are available below and who is responsible for compliance with the conditions of the lawful processing of personal information and other provisions of POPIA;
- (g) This Policy has been put in place throughout the Legoux Pty Ltd. and training on this policy will take place before the 1<sup>st</sup> of July 2021;
- (h) We have done a risk assessment to determine the possible risk factors and will make sure that we do everything to prevent the risk from occurring;
- (i) We have identified the role players and appointed the correct people to safeguard your information.
- (j) We have the following policies in place to protect our clients data:
  - A policy signed by all employees, with regards to the confidentiality of personal information and how to safeguard data subject's information as well as incident response.
  - PAIA & POPIA Manual;
  - POPIA Policy;

- Awareness Training and risk Assessment;
- Implemented access control;
- We have proper non-disclosure agreements and Service Level Agreements in place;
- We have security in place with regards to the access to our Building. Our clients can only access through the front door, where they will need to report to reception before entering the rest of the building. No client will have access to the building without the supervision of one of our employees. No maintenance will be done without supervision. We have an alarm system and cameras around the premises.
- We have an internal cleaning crew, who receives training on the importance of documents and they also sign a confidentiality agreement.
- All paperwork that is not necessary to file, will be destroyed by means of shredding.
- All files are stored in a storage room and all original documents of a significant value are stored in a safe. We have filing personnel who make sure that the files are stored safely and correctly. They are also bound by a confidentiality agreement. They will only take a file from the filing room to an employee when there is a specific task that needs to be completed and thereafter the file will be filed again.
- We make use of offsite storage for all our archived files that need to be kept in terms of the laws of South Africa for a certain period of time, before it can be destroyed. It is kept at an offsite facility which adheres to the required legislation and we have access thereto upon request.
- There is certain rules and procedures in place with regards to the use of USB, external hard drives and mobile devices by our employees. All devices used for collection and processing of personal information needs to be password protected.

## **11. PROCESSING OF PERSONAL INFORMATION**

We take the protection of our clients and employees personal information seriously and will only request and process the personal information in terms of POPIA. We process our data subject's personal information to provide them with a service and will be done with their consent. We treat all information as confidential.

If a data subject appoints us for a service, they agree that we may process their personal information. Categories of data subjects and personal information processed by Legoux Pty Ltd . includes but are not limited to:

(a) Clients and potential Clients:

- Name, surname and contact details;
- Company details;
- Bank details and/or Bank Statements depending on the service rendered;
- Tax Certificates from various entities;
- Tax and Financial Information;
- Copy of their Identity Document;
- Copy of their Proof of Address;
- List of employees with their details and payroll information;
- Biometric details if applicable.

(b) Suppliers:

- Company details;
- Contact details;
- Supplier Contracts;
- Bank Details
- Biometric information if applicable;
- Personal information of supplier representative.
- VAT Number;
- Registration Certificate / Registration Number;

(c) Shareholders:

- Contact details;
- Proof of address;
- Banking details;
- Copy of their Identification Document / Identification number.

(d) Employees:

- Name, Surname and contact details;
- Medical Information;
- Disability Information;
- Biometric Information;
- Pension and Provident Fund Information;
- Bank Details;
- Tax and financial Information;
- Employee Contracts;
- Vehicle Registration;
- Performance Records;
- Payroll Records;
- Electronic Access records;
- Physical access Records;
- Surveillance Records;
- Health and Safety Records;
- Training Records;
- Educational Records;
- Employment History;
- Personal information of family members;
- Copy of Identification Records.
- Race, Age and Sex.
- Criminal checks;
- Credit records;
- Disciplinary steps/processes taken.

(e) Job Applicants:

- CV (Curriculum Vitae);
- Criminal Checks;
- References;
- Credit Checks if applicable;
- Biometric information if applicable.

- Race, age and sex.

(f) Visitors:

- Name, Surname, contact details and Identification number.
- Physical access records;
- Electronic access records;
- Surveillance records.

## **12. DETAILS OF THE INFORMATION OFFICER & DEPUTY INFORMATION OFFICER**

Information Officer:           Roedolf Gouws  
Telephone No.:                011 475 1414  
Postal Address:                2 Pierre Rouge, Wildeperske Street, Westonaria, 1779  
Physical Address:              Unit C7, Westwood Office Park,  
  Allensnek, Roodepoort, 1724  
E-mail Address:                [rgouws@legouxsa.com](mailto:rgouws@legouxsa.com)

Deputy Information Officer: Tobie Gouws  
Telephone No.:                011 475 1414  
Postal Address:                2 Pierre Rouge, Wildeperske Street, Westonaria, 1779  
Physical Address:              Unit C7, Westwood Office Park,  
  Allensnek, Roodepoort, 1724  
E-mail Address:                tgouws@legouxsa.com