LA GRATITUDE OFFICES,
97 DORP STR, STELLENBOSCH, 7600
P O BOX 1559, STELLENBOSCH, 7599
TEL: +27 21 886 5262 • FAX: +27 21 886 6239

WWW.169ONMAIN.CO.ZA

169 ON MAIN (PTY) LTD: POLICY IN TERMS OF

THE PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013 ("POPIA")

Protecting the personal information of our clients is important to us.
169 On Main (Pty) Ltd is committed to processing your personal information in compliance with POPIA.

1. GENERAL

1.1 We take the utmost care to treat all client and employee information as strictly confidential.

1.2 We will only request your personal information for business purposes and process it with your consent.

1.3 The specific purpose/s for the collection, processing and storing of the personal information we request will be explained to you before it is collected, processed or stored.

1.4 We will request proof of identity before granting access to your record of personal information with us.

1.5 We will also ask for proof of identity should you wish to amend/update your record with us.

2. INFORMATION OFFICER

2.1 The details of our Information Officer, and Deputy Information Officers, are as follows:

Scholtz Conradie (Information Officer)

021 886 5262

scholtz@aaam.co.za

Robyn Clements (Deputy Information Officer)

021 886 5262

robyn@aaam.co.za

Helena du Plessis

021 886 5262

helena@aaam.co.za

2.2 For any queries relating to our data processing practices, please contact our Information Officer, or either of our Deputy Information Officers.

3. INCIDENT MANAGEMENT

3.1 We do everything we reasonably can, as required by POPIA, to protect your personal information. However, the risk of possible security breaches is still present, especially when it comes to electronically transferred data.

3.2 In instances where we become aware of a data security breach / possible data security breach, this will be reported to the Information Regulator, as well as to the data subject concerned, as soon as reasonably possible after becoming aware of the breach / potential breach, and, in terms of POPIA, we will provide enough information to allow the data subject to take action against any potential consequences.

4. EMPLOYMENT APPLICATIONS

4.1 All prospective employees are required to furnish the personal information, necessary for the processing of their employment applications, as well as for the purposes of background and reference checks.

4.2 Applicants confirm that, by supplying us with reference information, they have obtained the consent of the named reference.

5. EMPLOYEE COMPLIANCE WITH POPIA

5.1 Abacus employees who work with the personal information of our clients are required to attend a POPIA training workshop on how to deal with personal information in accordance with the provisions of POPIA, thereby ensuring that each employee is aware of the requirements for lawful processing of data.

5.2 Our Information Officer is responsible for updating and informing the employees of any relevant new regulations pertaining to POPIA and ensuring that they carry out their duties in line therewith.

6. DOCUMENTS AND FILES CONTAINING PERSONAL INFORMATION

6.1 Client and employee data is stored using One Drive and SharePoint on Microsoft Office.

6.2 The majority of the in-and-outflow of our client data is done via email. We do everything in our power to protect the data contained in this correspondence.

6.3 Only employees hold passwords for access to the firm's computers, which passwords are not shared with any other person.

6.4 Upon termination of employment, all forms of access to computers / printers / servers, etc. by password or otherwise, are removed by our IT agent.

6.5 Documents that are printed in hard copy are immediately removed from the printers and filed.

6.6 No physical or electronic files and/or documents containing client or employee personal information leaves our offices, situated at La Gratitude Offices, 97 Dorp Street, Stellenbosch, without the relevant insertion and signature into our "outgoing courier and control log book."

6.7 Further, removal of files/documents from the office building may only take place where it is done for work purposes and it has been determined, by a director, that the files/documents will not fall into the hands of an unauthorised person.

6.8 We make use of reliable courier services when documents need to be sent by courier and the documents are handed to the courier service in a sealed envelope.

6.9 Where employees work from home, remote access is granted to such employees, with the requisite security safeguards (passwords, etc.) in place.

6.10 Before an employee may remove his/her computer, or any component of the machine, from the office building, the consent of a director is required.

7. OFFICE ACCESS RESTRICTIONS

7.1 All physical and electronically created documents containing personal information are kept within the premises known as La Gratitude Offices, 97 Dorp Street, Stellenbosch / on devices within our ownership and control.

7.2 All physical files are kept in filing cabinets, which are locked at the end of each day.

7.3 After the expiry of the retention period, and where documents are not being further retained for record-keeping and/or auditing purposes, with the client's consent or in terms of tax legislation, the Information Officer ensures that such documents/files (electronic or physical) are properly destroyed (i.e., removed from our server or shredded, whichever is applicable).

8. BUILDING ACCESS

8.1 The doors and security gates to the office building are kept locked. Only authorised employees have access. The sliding doors to the building are controlled by a tag. All staff members have a tag, which is used to access the building and office.

8.2 The office building is further protected by an alarm-system, the passcode to which only authorised employees have access. The last director / employee to leave the premises is responsible for activating the alarm. We make use of an application which enables the directors to have sight of who is arming and disarming the alarm and when, as well as who is entering and leaving the building.

9. RISK AWARENESS

9.1 A risk analysis is conducted annually, where we do a thorough inspection of our existing security measures.

9.2 Where necessary, the relevant aspects of our security is updated to ensure the strongest possible security measures, safeguarding both the physical and electronic documents/files containing personal information of clients and employees, are in place.

10. SUB-CONTRACTORS

10.1 There are a number of instances where we, with the prior consent of the client, must make use of a sub-contractor, real estate agents, building contractors, attorneys, etc.

10.2 These sub-contractors are obliged to treat our client and employee data with the same level of confidentiality as we do, in terms of a signed confidentiality agreement.

10.3 Where a sub-contractor handles client information in a manner contrary to the provisions of our privacy and POPIA policies, or there are reasonable grounds to believe that a sub-contractor has handled client information in a manner contrary to the provisions of our privacy and POPIA policies, this will be reported to the data subject concerned, as well as to the Information Regulator, by our Information Officer.

11. BACK-UP SUPPORT

11.1 All electronic data is saved on our cloud-based system, OneDrive and SharePoint on the Microsoft Business program.

11.2 The Microsoft "cloud-based" system, which is used to store our data is governed by the Personal Information International Disclosure Protection Act. Shares are also set up based on permissions and roles within the company and accessed using Multi Factor authentication.