KABOD DEVELOPMENT GROUP (PTY) LTD: POLICY IN TERMS OF

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

The Kabod Development Group (Pty) Ltd ("The Kabod Group") is committed to compliance with POPIA and protecting the personal information entrusted to us by our clients and employees.

1. GENERAL

1.1 The Kabod Group treats all client and employee information with utmost care and regard to confidentiality.

1.2 We will only request your personal information for the purposes of conducting our business and carrying out our mandate/instructions, and the information you provide to us will be processed only with your knowledge and consent.

1.3 We undertake to explain the specific reasons for requesting and processing your personal information upfront, and where that same information is / needs to be processed for a further reason, we will obtain your further consent before doing so.

1.4 Where you request access to your personal information we hold, we will first ask for proof of identity before granting such access.

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

1.6 A request for confirmation of whether we hold your personal information is done free of charge. However, where you request a record or description of your personal information we have, the prescribed fee (if any) will be charged and your request will be attended to within a reasonable time.

2. INFORMATION OFFICER

2.1 The details of our Information Officer are as follows:
Gideon Roos
083 657 9856
groos@kabodgroup.co.za

2.2 The details of our Deputy Information Officer are as follows:
Chantell Roos
079 881 7748
sales@bretagnaestate.com

2.3 For any queries relating to our data processing practices, please contact our Information Officer / Deputy Information Officer.

3. INCIDENT MANAGEMENT

3.1 We do everything we reasonably can to protect your personal information. However, we cannot entirely eliminate the risk of a breach of security of personal information, especially when it comes to cyber security and electronically transmitted data.

3.2 Where we become aware of a data security breach / have reasonable grounds to believe that there has been a 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 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 certain personal information, necessary for the processing of their employment applications for the purposes of background and reference checks.

4.2 Applicants confirm that the details of references provided to us are so furnished with the express consent of the named reference.

5. EMPLOYEE COMPLIANCE WITH POPIA

5.1 Employees of The Kabod Group are required to attend a POPIA training workshop on how to deal with the personal information of clients in line with the provisions of POPIA. Therefore, it is ensured that every employee is aware of the requirements for lawful processing of personal information and is bound to treat all client information as confidential.

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 CONTAINING PERSONAL INFORMATION

6.1 Client and employee data is stored using the "Hubspot" and "PropData" processing and storage packages.

6.2 The majority of the in-and-outflow of our client data is done via email, and in some instances, WhatsApp or SMS messaging. However, personal information of a sensitive / confidential nature is rarely shared on these short messaging services. In the event that personal information is shared on WhatsApp or by sms, only our sales agent has access to the

communication, and the mobile phone and computer used for this correspondence are both password protected.

6.3 Emails that contain personal information are sent with password protection and can only be accessed by the recipient / person whose email account it is.

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

6.5 Upon termination of employment, all forms of access to computers / printers / servers, etc. by password or otherwise, are removed by our IT agent within twelve (12) hours of termination of service.

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

6.7 No physical or electronic files and/or documents containing client or employee personal information leaves our office, located at Farm 26158, Wemmershoek Road (R301), Paarl, without the prior knowledge and approval of a director.

6.8 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.

6.9 Where employees are required to work from home, remote access is granted to such employees, with the requisite security safeguards (passwords, etc.) in place. Devices and accounts containing personal information that are used by employees to work from home are also password-protected.

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 Farm 26158, Wemmershoek Road (R301), Paarl.

7.2 All physical files are kept in filing cabinets, which are locked at the end of each day. The filing cabinets are kept in a locked room within the office building. Only the Information Officer and Deputy Information Officer have access to the room in which the filing cabinets are kept.

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. The Deputy Information Officer personally sees to the shredding of documents containing personal information.

8. BUILDING ACCESS

8.1 The doors and security gates to the office building are kept locked at all times. Only authorised employees have access to / a copy of the key.

8.2 The office building is further protected by an alarm-system and armed response, the passcode to which only authorised employees have access. The last employee to leave the premises is responsible for activating the alarm.

8.3 Access to the office building is monitored by CCTV-cameras and a 24-hour security service.

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.

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 Where necessary, our data is stored on an external hard drive and kept in a locked safe, which safe is kept in a locked room in our office building.

11.2 Only the Information Officer and Deputy Information Officer will have access to this safe.