


MULTIMEDIA VILLA
COMPLIANCE MANUAL
FOR THE IMPLEMENTATION OF THE
PROTECTION OF PERSONAL INFORMATION ACT OF 2013

A large, semi-transparent watermark of the Multimedia Villa logo is centered behind the text. The logo features a stylized 'M' composed of several small circles on the left, followed by the words 'Multimedia VILLA' in a sans-serif font. The 'Multimedia' part is in a light orange color, and 'VILLA' is in a light grey color.

1. INTRODUCTION

The Protection of Personal Information Act (POPI) is intended to balance 2 competing interests. These are:

- 1.1. Individual constitutional rights to privacy; and
- 1.2. The needs of society to have access to and to process personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for MULTIMEDIA VILLA's compliance with POPI.

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

2. UNDERTAKINGS TO CLIENTS:

The company undertakes to follow POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of clients.

- 2.1 The company undertakes to process information only for the purpose for which it is intended.
- 2.2 Whenever necessary, the company shall obtain consent to process personal information.
- 2.3 Where the company does not seek consent, the processing of client's personal information will be following a legal obligation, or to protect a legitimate interest that requires protection.

- 2.4 The company shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.
- 2.5 The shall collect personal information directly from the client whose information is required, unless:
- 2.5.1 the information is of public record, or
 - 2.5.2 the client has consented to the collection of their personal information from another source, or
 - 2.5.3 the collection of the information from another source does not prejudice the client, or
 - 2.5.4 the information to be collected is necessary for the maintenance of law and order or national security, or
 - 2.5.5 the information is being collected to comply with a legal obligation, including an obligation to SARS, or
 - 2.5.6 the information collected is required for the conduct of proceedings in any court or tribunal, where these proceedings have commenced or are reasonably contemplated; or
 - 2.5.7 the information is required to maintain legitimate interests; or
 - 2.5.8 where requesting consent would prejudice the purpose of the collection of the information; or
 - 2.5.9 where requesting consent is not reasonably practical in the circumstances.
- 2.6 The shall advise clients of the purpose of the collection of the personal information.
- 2.7 The company shall retain records of the personal information tha has been collected for the minimum period as required by law unless the client has furnished their consent or instruction to retain the records for a longer period.
- 2.8 The company shall destroy or delete records of the personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which the records are to be held has expired.
- 2.9 The Company shall restrict the processing of personal information:

- 2.9.1 where the accuracy of the information is contested, for a period sufficient to enable verification the accuracy of the information;
 - 2.9.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;
 - 2.9.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or
 - 2.9.4 where the client requests that the personal information be transmitted to another automated data processing system
- 2.10 The further processing of personal information shall only be undertaken:
- 2.10.1 if the requirements of paragraphs 3; 6.1; 6.4; 6.5 or 6.6 above have been met;
 - 2.10.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;
 - 2.10.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or
 - 2.10.4 where this is required by the Information Regulator appointed in terms of POPI.
- 2.11 The Company undertakes to ensure that the personal information collected and process is complete, accurate, not misleading and up to date.
- 2.12 The company undertakes to retain the physical file and the electronic data related to the processing of the personal information.

3. CLIENT'S RIGHTS

- 3.1 In cases where the client's consent is required to process their personal information, this consent may be withdrawn.
- 3.2 In cases where personal information is processed without consent to protect a legitimate interest, to comply with the law or to pursue or protect legitimate interests, the client has the right to object to such processing.

3.3 All clients are entitled to lodge a complaint regarding the application of POPI with the Information Regulator.

4. SECURITY SAFEGUARDS

In order to secure the integrity and confidentiality of the personal information in the possession of the company, and to protect it against loss or damage or unauthorised access, the following security safeguards shall be implemented

- 4.1 The business premises where records are kept must remain protected by access control, burglar alarms and armed response.
- 4.2 Archived files must be stored behind locked doors and access control to these storage facilities must be implemented.
- 4.3 All the user terminals on the internal computer network and servers must be protected by passwords which must be changed on a regular basis.
- 4.4 All email infrastructure must comply with industry standard security safeguards, and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.
- 4.5 Vulnerability assessments must be carried out on digital infrastructure at least on an annual basis to identify weaknesses in the company's systems and to ensure that adequate security is in place.
- 4.6 The Company must use an internationally recognised Firewall to protect the data on local servers. The security of this system must comply with the GDPR of the European Union.
- 4.7 Members of the staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.
- 4.8 It must be a term of the contract with every staff member that they must maintain full confidentiality in respect of all of clients' affairs.
- 4.9 Employment contracts for staff whose duty it is to process a client's personal information, must include an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person. See form O. 6 below for an example of the relevant addendum/clause to be used in these contracts.

- 4.10 The processing of the personal information of staff members must take place in accordance with the rules contained in the relevant labour legislation.
- 4.11 The digital work profiles and privileges of staff who have left out employ must be properly terminated.
- 4.12 The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.
- 4.13 These security safeguards must be verified on a regular basis to ensure effective implementation, and these safeguards must be continually updated in response to new risks or deficiencies.

5. SECURITY BREACHES

- 5.1 Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, a notification will be sent to the the Information Regulator and the relevant clients.
- 5.2 Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed
- 5.3 The notification to the client must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:
 - 5.3.1 by mail to the client's last known physical or postal address;
 - 5.3.2 by email to the client's last known email address;
 - 5.3.3 by publication on the company website or in the news media; or
 - 5.3.4 as directed by the Information Regulator.
- 5.4 This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:
 - 5.4.1 a description of the possible consequences of the breach;
 - 5.4.2 details of the measures that will be taken to address the breach;
 - 5.4.3 the recommendation of what the client could do to mitigate the adverse effects of the breach; and

5.4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

6. CLIENTS REQUESTING RECORDS

6.1 On production of proof of identity, any person is entitled to request confirmation, free of charge, whether or not the company holds any personal information about that person in its records.

6.2 If the company has stored such personal information, on request, and upon payment of a fee of R200 a description of the personal information will be provided to the person, including information about the identity of all third parties or categories of third parties who have or have had access to the information.

6.3 A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form.

6.4 In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.

6.5 If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed.

7. THE CORRECTION OF PERSONAL INFORMATION

7.1 A client is entitled to require the company to correct or delete personal information that is on record, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

7.2 A client is also entitled to require the company to destroy or delete records of personal information about the client that is no longer lawfully retained.

7.3 Any such request must be made on the prescribed form

7.4 Upon receipt of such a lawful request, the company must comply as soon as reasonably practicable.

7.5 In the event that a dispute arises regarding the client's rights to have information corrected, and in the event that the client so requires, the company must attach to the information, in a way that it will always be read with the information, an indication that the correction of the information has been requested but has not been made.

7.6 A notification will be provided to the client who has made a request for their personal information to be corrected or deleted what action has been taken as a result of such a request.

8. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

8.1 The Company may only process the personal information of a child if the consent of the child's parent or legal guardian has been obtained.

9. INFORMATION OFFICER

9.1 The Company's appointed Information Officer is **Brian Makwaiba** who is the Chief Executive Officer. The Information Officer's responsibilities include:

9.1.1 Ensuring compliance with POPI.

9.1.2 Dealing with requests received in terms of POPI.

9.1.3 Working with the Information Regulator in relation to investigations.

9.2 The Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above.

9.3 The Information Officer and the Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties,

9.4 In carrying out their duties, the Information Officer must ensure that:

9.4.1 this Compliance Manual is implemented;

- 9.4.2** a Personal Information Impact Assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
- 9.4.3** that this Compliance Manual is developed, monitored, maintained and made available;
- 9.4.4** that internal measures are developed together with adequate systems to process requests for information or access to information;
- 9.4.5** that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and
- 9.4.6** that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator)

9.5 Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and the Information Officer and deputy Information Officers must familiarize themselves with the content of these notes.



10. PRIOR AUTHORISATION

In the following circumstances, the company will require prior authorisation from the Information Regulator before processing any personal information:

- 10.1 Where information is going to be intend to utilised (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of internal processing) for any purpose other than the original intention, or to link the information with information held by others;
- 10.2 processing information on criminal behaviour or unlawful or objectionable conduct;
- 10.3 processing information for the purposes of credit reporting
- 10.4 transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

10.5 The Information Regulator must be notified of the intention to process any personal information as set out in above above prior to any processing taking place and no processing is to commence until the Information Regulator has decided in favour of such processing

11. DIRECT MARKETING

direct marketing (using any form of electronic communication) may only go out to clients to clients if:

11.1.1 they were given an opportunity to object to receiving direct marketing material by electronic communication at the time that their personal information was collected; and

11.1.2 they did not object then or at any time after receiving any such direct marketing communications from us

11.2 a person may be approached to ask for their consent to receive direct marketing material only once, no such approach may happen if they have previously refused their consent.

11.3 A request for consent to receive direct marketing must be made in the prescribed manner and form

11.4 All direct marketing communications must disclose the company's identity and contain an address or other contact details to which the client may send a request that the communications cease.

12. TRANSBORDER INFORMATION FLOWS

The company may not transfer a client's personal information to a third party in a foreign country, unless:

12.1 The client consents to this, or requests it; or

12.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country; or

12.3 the transfer of the personal information is required for the performance of the contract between the company and the client; or

12.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between the

company and the third party; or the transfer of the personal information is for the benefit of the client and it is not reasonably possible to obtain their consent and that if it were possible the client would be likely to give such consent.

13. OFFENCES AND PENALTIES

- 13.1** POPI provides for serious penalties for the contravention of its terms. For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.
- 13.2** Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

