**TURNER MORRIS (PTY) LTD T/A**
**TURNER MORRIS**
**AFM**
**AUTO BUILD**
**SURVEY INSTRUMENTS**

# POPIA FRAMEWORK (BINDING CORPORATE RULES)

## 1. SCOPE AND APPLICATION

### 1.1 Scope

This Framework addresses the Processing of Personal Data of employees, customers and suppliers by or on behalf of Turner Morris in their role as a Responsible Party. This Framework complies with the privacy objectives and principles housed under the Protection of Personal Information Act, 4 of 2013 (hereinafter referred to as "POPIA").

### 1.2 Effective Date

This Framework comes into effect as of 01 June 2021.

### 1.3 Application

This Framework applies to the Processing of Personal Information by electronic means and in paper-based filing systems. This Framework is binding on Turner Morris in respect of their Processing of Personal Information within the company.

## 2. INTERPRETATION

### 2.1 Definitions

The following are the meanings of defined terms used in this Framework:

**"Personal Information"** is information or data about an identified or identifiable living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to— (a) Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; (b) Information relating to the education or the medical, financial, criminal or employment history of the person; (c) Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; (d) The biometric information of the person; (e) The personal opinions, views or preferences of the person; (f) Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; (g) The views or opinions of another individual about the person; and (h) The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person, received by the Responsible Party from any party in any format including, without limitation, electronic, paper, and verbal;

**"Data Subject"** is the individual who is the owner of the Personal Information;

**"Processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including— (a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; (b) Dissemination by means of transmission, distribution or making available in any other form; or (c) Merging, linking, as well as restriction, degradation, erasure or destruction of information. Processing includes any online and offline processing and includes such activities as copying, filing, and inputting Personal Information into a database;

**“Responsible Party/ies”** means the party who determines the purpose of and means for processing Personal Information, and shall refer to Turner Morris.

**"Special Personal Information"** is information or data about an individual that pertains to racial or ethnic origins, political or religious beliefs, health, or sexual orientation or preferences, biometric data and data regarding minors. Special Personal

Information may not be processed at all unless the individual has given explicit consent.

## 3. DATA PROTECTION PRINCIPLES

In Processing Personal Information, the Responsible Party shall comply with the eight conditions for the lawful processing of personal information in terms of POPIA (the "Conditions").

Adherence to the Conditions may be limited in certain cases to the extent necessary to meet national security, public interest, or law enforcement requirements.

The Conditions are as follows:

3.1 Condition 1 – Accountability:

3.1.1 The party collecting the Personal Information must ensure compliance with the principles of POPIA.

3.2 Condition 2 – Processing Limitation:

3.2.1 Personal Information can be collected or stored only if it is necessary for, or directly related to, a lawful, explicitly defined purpose and does not intrude on the privacy of the consumer to an unreasonable extent.

3.2.2 Personal Information must be collected directly from and with the consent of the consumer.

3.3 Condition 3 – Purpose Specification:

3.3.1 Consumers must be informed of the purpose of any such collection and of the intended recipient of the Personal Information at the time of collection.

3.3.2 Personal Information must not be kept for any longer than is necessary for achieving the purpose for which it was collected.

3.4 Condition 4 – Further Processing Limitation:

3.4.1 Personal Information must not be distributed in any way which is incompatible with the purpose for which it was collected.

3.5 Condition 5 – Information Quality:

3.5.1 Reasonable steps must be taken to ensure that the Personal Information processed is accurate, up to date and complete.

3.6 Condition 6 – Openness:

3.6.1 The Data Subject whose information you are collecting must be aware that you are collecting and processing their Personal Information.

3.6.2 They must be notified of the fact either before or as soon as reasonably possible after collection of the Personal Information, even if you get it from a third party.

3.7 Condition 7 – Security Safeguards:

3.7.1 Appropriate technical and organisation measures have to be taken to safeguard the consumer against the risk of loss, damage, destruction of or an authorised access to Personal Information.

3.8 Condition 8 – Data Subject Participation:

3.8.1 Consumers are allowed the right to access their Personal Information and have a right to demand correction of such information should it turn out to be inaccurate.

3.9 **Personal Information Collected**

3.9.1 The type of Personal Information collected will depend on the purpose for which it is collected and will be processed for that purpose only. The Personal Information that Turner Morris collects and processes falls into three broad categories:

3.9.1.1 Human Resources data;

3.9.1.2 Procurement data; and

3.9.1.3 Customer/Consumer data.

3.9.2 Wherever possible, the Responsible Party will inform the Data Subject what information he/she/it is required to provide to it and what information is optional.

3.10 **Purpose for Processing Personal Information**

3.10.1 Personal Information shall be collected, used, transferred or otherwise Processed for one or more of the following purposes:

3.10.1.1 The conclusion and execution of agreements with customers and suppliers;

3.10.1.2 Marketing, sales, and promotions;

3.10.1.3 Account management;

3.10.1.4 Customer service;

3.10.1.5 Finance and accounting;

3.10.1.6 Procurement;

3.10.1.7 External communications;

3.10.1.8 Compliance with a legal obligation.

3.11 **How Personal Information Is Used**

3.11.1 Personal Information is only to be used for the purpose for which it was collected and agreed to be used for.

3.11.2 The Responsible Party shall notify all identified Data Subjects about the purposes for which Personal Information is collected and used. In certain situations, data is aggregated or "made anonymous" so that the names of the Data Subjects are not known by data processors within Turner Morris. In these cases, Data Subjects do not need to be notified.

3.11.3 The Responsible Party must give each Data Subject the opportunity to opt out from allowing them to disclose his/her Personal Information to a third party. Affirmative choice (opt-in) must be given if Special Personal Information is to be disclosed to a third party.

3.11.4 A Data Subject must positively agree to the use of his/her/its Personal Information for a purpose incompatible with the purpose for which it was originally collected or authorized.

3.12 **Consent**

3.12.1 Whenever Personal Information is collected, the Responsible Party must ensure that the Data Subject is made aware of:

3.12.1.1 the information being collected and where the information is not collected from the Data Subject, the source from which it is collected;

3.12.1.2 the name and address of the Responsible Party;

3.12.1.3 the purpose for which the information is being collected;

3.12.1.4 whether or not the supply of the information by that Data Subject is voluntary or mandatory;

3.12.1.5 the consequences of failure to provide the information;

3.12.1.6 any particular law authorising or requiring the collection of the information;

3.12.1.7 the fact that, where applicable, the Responsible Party intends to transfer the information to a third country or international organisation (e.g., for off-shore server storage) and the level of protection afforded to the information by that third country or international organisation;

3.12.1.8 the recipient or category of recipients of the information;

3.12.1.9 the nature or category of the information;

3.12.1.10 the existence of the right of access to and the right to rectify the information collected;

3.12.1.11 the existence of the right to object to the Processing of Personal Information; and

3.12.1.12 the right to lodge a complaint with the Information Regulator and the contact details of the Information Regulator.

3.13 **Disclosure of Personal Information**

The Responsible Party may transfer information to a third party acting as an agent for the Responsible Party (such as an outside benefits administrator). However, prior to any such transfer, the Responsible Party must require the third party to give its written agreement to provide the same level of protection required by the Conditions. If possible, a Third-Party Operator Agreement shall be concluded between the Responsible Party and its agent.

3.14 **Direct Marketing**

3.14.1 When Processing Personal Information for the purpose of making direct marketing communications, the Responsible Party will either:

3.14.1.1 obtain the prior affirmative consent ("opt-in") of the targeted consumer; or

3.14.1.2 ensure that it only Processes the Personal Information of consumers who are customers of the Responsible Party who have not previously chosen not to receive such communications.

3.14.2 In every subsequent direct marketing communication that is made to the individual, the individual shall be offered the opportunity to opt-out of further marketing communication.

3.15 **Safeguarding Personal Information**

3.15.1 The Responsible Party must take reasonable precautions to protect Personal Information from loss, misuse, unauthorized access, disclosure, alteration, and destruction. These precautions include password protections for online information systems and restricted access to Personal Information processed by the Responsible Party.

3.15.2 All inquiries, whether written or verbal, concerning any Personal Information, are to be referred to the Information Officer/Chief Executive Officer of the Responsible Party for handling. The Responsible Party will verify the credentials of the inquirer and obtain the Data Subject's consent before releasing information about a Data Subject.

3.16 **Access and Correction of Personal Information**

Upon request, Data Subjects may access Personal Information about themselves and request that inaccurate or incomplete information be corrected or amended.

3.17 **Complaints**

The Responsible Party shall implement a complaint management process and apply consistent incident management procedures from identification through to resolution. Complaints shall be submitted through the following mechanisms:

3.17.1 Online - Complaints must be submitted via the “Contact Turner Morris” form on the Responsible Party’s website.

3.17.2 Telephone - Complaints can be reported via telephone using the telephone number provided on the Responsible Party’s website.

Upon receipt of a complaint, the Responsible Party will review the submission and investigate the complaint. The Responsible Party will acknowledge receipt of a complaint within ten business days and will respond to all submissions within twenty business days.

3.18 **Retention of Personal Information**

3.18.1 Purpose

3.18.1.1 To exercise effective control over the retention of documents and electronic transactions as prescribed by legislation and as dictated by business practice.

3.18.1.2 Documents need to be retained in order to prove the existence of facts and to exercise any rights that the Responsible Party may have. They are also necessary for defending legal action, for establishing what was said or done

in relation to the business of the Responsible Party and to minimize the Responsible Party's reputational risks.

3.18.1.3 To ensure that the Responsible Party's interests are protected and that the Responsible Party and the Data Subjects' rights to privacy and confidentiality are not breached.

3.18.1.4 Queries may be referred to the Information Officer or Chief Executive Officer of the Responsible Party.

3.18.2 Retention Period

The Responsible Party must strive to keep Personal Information only for the time necessary for the purposes set out in this Framework and in accordance with the law. As a general rule:

3.18.2.1 The Data Subject's data will be kept for three years from the date of collection or after the last contact or the end of the commercial relationship, unless opposed by the Data Subject. At the end of this three-year period, the Responsible Party may make contact with the Data Subject again in order to find out whether or not the Data Subject wishes for the Responsible Party to continue to retain his/her/its Personal Information. If no clear positive answer is given by the Data Subject, his/her/its data will be deleted or archived in accordance with POPIA.

3.18.2.2 Data that is required to prove a right or a contract or to be kept under compliance with a legal obligation can be archived in accordance with the law.

3.19 **Destruction of records/documents**

3.19.1 Records of Personal Information must be destroyed after the termination of the retention period. The Information Officer/Chief

Executive Officer of the Responsible Party will request the party/ies dealing with the Personal Information to attend to the destruction of its documents and these requests shall be attended to as soon as possible.

3.19.2 Each Responsible Party is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain whether 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 Responsible Party pending such return.

3.19.3 After completion of the process in 3.19.2 above, the Information Officer/ Chief Executive Officer of the Responsible Party shall, in writing, authorise the removal and destruction of the records/documents.

3.19.4 Documents/records may also be stored off-site, in storage facilities approved by the Responsible Party. However, should the off-site storage be outside the Republic of South Africa, the Data Subject must have consented to the transfer.

3.20 **Data Integrity**

The Responsible Party shall take reasonable steps to ensure that Personal Information is accurate, complete, and current. All Data Subjects are asked to inform the Responsible Party immediately in the event of changes in Personal Information.

3.21 **Security Breach**

3.21.1 A security breach occurs when the data for which the Responsible Party is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity.

3.21.2 If a security breach occurs, the following protocol is to be observed:

3.21.2.1 The Responsible Party's IT officer is to isolate the incident and complete a breach report.

3.21.2.2 The IT officer is to provide the report and notify the Information Officer/Chief Executive Officer together with the Managing Director of the Responsible Party.

3.21.2.3 The Information Officer of the Responsible Party must notify the Information Regulator in South Africa without undue delay, and at the latest within 72 hours after having become aware of the security breach.

3.21.3 The notification must:

3.21.3.1 Describe the nature of the breach;

3.21.3.2 State the number of the Data Subjects affected by the breach;

3.21.3.3 Describe the likely consequences of the breach; and

3.21.3.4 Describe the measures taken or proposed to be taken by the Responsible Party to remedy the breach.

3.21.4 If it is likely that the breach poses a risk to a Data Subject's rights, then the Data Subject should also be informed, unless there are effective technical and organisational protection measures that have been put in place, or other measures that ensure that the risk is no longer likely to materialise or the Data Subject cannot be identified.

## 4. TURNER MORRIS' COMMITMENTS

### 4.1 Governance

4.1.1 Turner Morris' Information Officer is chartered to ensure compliance with POPIA and is responsible for overseeing compliance of its Framework. The Information Officer shall provide regular reports to Turner Morris' Board of Directors.

### 4.2 Training

4.2.1 Turner Morris shall provide general POPIA training to its staff in order to address the compliance obligations under this Framework.

4.2.2 Depending on business needs, risk assessment outcomes, assurance processes and other factors, Turner Morris shall develop and refresh the training periodically and may develop additional training programs.