

## 5. Policy: Data Operators

### 5.1. PURPOSE

The control of risks introduced into the Company by contractors, service providers, accountants, consultants, third-parties and suppliers (Data Operators) is an important element of the Company risk management system. For the purposes of this Policy Data Operator means any organisation whom the Company pays in return for any type of goods or service, or the processing of Personal Information. Selection criteria for Data Operators are dependent on the nature of the goods or services to be supplied and are determined by the Company policies and procedures plus statutory requirements.

This Policy defines the duties of the Data Operator in terms of the processing of Personal Information on behalf of the Company in compliance with the Protection of Personal Information Act, No.4 of 2013.

This Policy must be read in conjunction with the *Acceptable Usage Policy*. Confidentiality Agreements and Non-Disclosure Agreements referred to in the *Acceptable Usage Policy*, will be found in the Annexure of this Policy as it relates to Data Operator Personal Information as well as processing of Personal Information by Data Operators (*Refer to Annexure C and D*)

### 5.2. INTRODUCTION

If the Company uses Data Operators to process Personal Information, it must comply with Sections 20 and 21 of the Protection of Personal Information Act. POPIA requires the Company to enter into a written agreement with a Data Operator that processes Personal Information for the Company. The Company must ensure that such Data Operator maintains the security measures required by POPIA.

### 5.3. GUIDANCE FOR REVIEWING & MONITORING DATA OPERATORS

#### **POPIA and Data Security Policies**

The first stage in the process is to see if the Data Operator has the right attitudes to the security of Personal Information, and this is done by checking their policies.

#### **Competence**

Next a check should be carried out to ensure that the Data Operator are capable of processing Personal Information in a responsible manner and supplying services that meet appropriate legal requirements.

#### **Standards**

Once it is established that Data Operator can work in accordance with POPIA requirements, the Company needs to check that the product or service the Data Operator will supply is of a high enough standard.

#### **Monitoring**

Checks on policies, competence and standards must take place before the Data Operator's 'offer' (usually a quote, whether verbal or written) is accepted by the Company. There will be a need to monitor Data Operators' work to ensure that they are complying with the agreed methods and risk control measures. Also, that execution of the service is performed in accordance with proposed methods and control measures. Verification of the service takes place throughout service delivery. These checks complete the selection process. As soon as verification that the purchased product or services meet specified POPIA requirements is completed, the Data Operator can then be contracted under the Company's existing day-to-day POPIA controls.

### 5.4. DATA OPERATOR DUTIES

The Data Operator agrees to the following (further details of which can be found in the section headed *Information Processing Agreement (Refer to Annexure E)*):

- Only use and disclose the Personal Information in accordance with the Company's specific written instructions.

Company Name: Calypso Creative Agency cc  
Company Reg Nr: 2009/194454/23  
Date: 23 June 2021

- Take reasonable and appropriate, organisational, and technical security measures to protect Personal Information supplied by the Company or otherwise made available to the Data Operator.
- Permit the Company to audit the Data Operator in terms of its compliance with Sections 19 to 21 of POPIA.
- Comply with requests by the Company for access to Personal Information following the receipt of a valid and approved Data Subject Request.

The Data Operator is not permitted to sub-contract any of the processing of the Personal Information supplied by the Company, without first:

- Ensuring the sub-contractor will be compliant with the requirements of Sections 19 to 21 of POPIA.
- Obtaining prior written permission of the Company.

The Data Operator must also agree to co-operate with any action required to fulfil the requests or demands of the Information Regulator as outlined in POPIA, whether directly by the Information Regulator or indirectly by the Company.

#### **5.5. RIGHTS OF THE COMPANY**

An audit of the compliance of the Data Operator with Sections 19 to 21 of POPIA to be conducted by the Company, may include but is not limited to:

- Ensuring that the Data Operator transfers data securely.
- Ensuring that the Data Operator reports any security breaches or other problems to the Company.
- In any other way fulfil the duties of the Company as outlined in Section 21 of POPIA.

#### **5.6. TERMINATION OF INFORMATION PROCESSING AGREEMENT**

In terms of processing of Personal Information:

- Where the Data Operator is found by the Information Regulator to have not fulfilled its obligations in terms of compliance with POPIA, the Company has the right to cancel the Information Processing Agreement with the Data Operator with immediate effect.
- Whether for fault or any other termination reason, the Data Operator must return all Personal Information processed on behalf of the Company without delay, unless the Data Operator is required to retain such records in terms of other legislation or regulations.

#### **5.7. RIGHTS RESERVED BY THE COMPANY**

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

#### 5.9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

#### 5.10. POLICY AWARENESS AND UPDATE

##### Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

##### Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

##### Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

#### 5.11. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Mrs Paula Gageiro		23 June 2021

#### 5.12. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes