CTP LIMITED

CTP Limited | Reg. No. 1971/004223/06 | (Formerly The Press Corporation of S.A. Ltd)

P.O. Box 43156
Industria
2042

2nd Floor
Citizen Building
9 Wright Street
Industria

Tel: 010-492-5359
Fax: 011-474-1495

# INFORMATION PROTECTION POLICY

## INDEX



## 1 INTRODUCTION

To meet the key functions, the Company recognises that it has to process the Personal Information of its employees, potential consumers, consumers and third parties. In doing so, the Company is committed to the observance of, and compliance with, the directives of the Constitution and national legislation alike, including the Protection of Personal Information Act. The Company endorses the key principles of good governance, transparency and accountability and seeks to regulate the use and Processing of Personal Information as lawfully required.

## 2 DEFINITIONS AND INTERPRETATION

### 2.1 Definitions

2.1.1 In this Policy, unless clearly inconsistent with or otherwise indicated by the context –

2.1.1.1 "**Company**" means Caxton and CTP Publishers and Printers Limited, a company incorporated in accordance with the laws of South Africa under registration number 1947/026616/06, and any of its subsidiaries;

2.1.1.2 "**Data Subject**" means the person or persons, whether juristic or natural, to whom or to which Personal Information relates and "**Data Subjects**" mean more than one Data Subject;

2.1.1.3 "**Designated Employees**" mean a natural person employed by the Company or any of its subsidiaries to Process the Personal Information of Data Subjects at the Company's direction or on its behalf and "**Designated Employees**" mean more than one Designated Employee;

2.1.1.4 "**Electronic Communications and Transactions Act**" means the Electronic Communications and Transactions Act, No. 25 of 2002, as amended from time to time;

2.1.1.5 "**Information Protection Officer**" means the person appointed by the Company to maintain the privacy and protection of Personal Information in terms of a duly executed letter of appointment, being the person listed in paragraph 13.4 of this Policy;

2.1.1.6 "**Processing**" means the operation or activity or manipulation of or set of operations, whether or not by automated means, concerning Personal Information, including -

2.1.1.6.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use of Personal Information;

2.1.1.6.2 the dissemination of Personal Information by means of transmission, distribution or making available in any form; or

2.1.1.6.3 merging, linking, as well as restriction, degradation, erasure or destruction of Personal Information.

2.1.1.7 "**Protection of Personal Information Act** " means the Protection of Personal Information Act, No. 4 of 2013, as amended from time to time;

2.1.1.8 "**Personal Information**" means information relating to an identifiable, living, natural person and, where it is applicable, information relating to an identifiable, juristic person, including –

2.1.1.8.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, sexual orientation, age, physical or mental health, wellbeing, disability, religion, belief, culture, language and place of birth of the person;

2.1.1.8.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.1.1.8.3 an identifying number, symbol, e-mail address, telephone number, location, online identifier or other particular assignment to the person;

2.1.1.8.4 the biometric information of the person;

2.1.1.8.5 the personal opinions, views or preferences of the person or the views or opinions of another individual about the person;

2.1.1.8.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal contents of the original correspondence; and

2.1.1.8.7 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;

2.1.1.9 "**Policy**" means this information protection policy, as amended from time to time, including the appendices attached hereto;

2.1.1.10 "**Record**" means recorded information –

2.1.1.10.1 regardless of the form or medium, including the following -

2.1.1.10.1.1 the writing of any material;

2.1.1.10.1.2 information produced, recorded or stored by means of a tape-recorder, computer equipment (whether through hardware or software or both) or other devices, and any material subsequently derived from information so produced, recorded or stored;

2.1.1.10.1.3 the labelling, marking or other writing that identifies or describes anything of which it forms part of, or which it is attached by any means to;

2.1.1.10.1.4 the booking, mapping, planning, graphing or drawing; or

2.1.1.10.1.5 photograph, film, negative, tape of other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

2.1.1.10.2 in the possession or under the control of a Responsible Party;

2.1.1.10.3 whether or not it was created by a Responsible Party; and/or

2.1.1.10.4 regardless of when it came into existence; and

2.1.1.11 "**Responsible Party**" means a public or private entity or any other person, which, either alone or in conjunction with others, has been contracted by the Company to determine the purpose of and means for Processing a Data Subject's Personal Information at the Company's direction or on its behalf.

2.2 **Interpretation**

2.2.1 Unless clearly inconsistent with or otherwise indicated by the context -

2.2.1.1 any reference to the singular includes the plural and *vice versa*;

2.2.1.2 any reference to natural persons includes legal persons and *vice versa*; and

2.2.1.3 any reference to a gender includes the other genders.

2.2.2 Words and expressions defined in any sub-clause shall, for the purposes of the clause of which that sub-clause forms part, bear the meanings assigned to such words and expressions in that sub-clause.

3 **APPLICABLE LAW**

3.1 The laws of the Republic of South Africa apply exclusively to this Policy. If a provision of this Policy is deemed illegal, void or unenforceable due to applicable law or order of a court of a competent jurisdiction, then that provision shall be deemed to have been deleted and the remaining provisions of this Policy will not be prejudiced and will continue in full force and effect.

3.2 No provision(s) of this Policy -

3.2.1 does or purports to limit or exempt the Company from liability (including liability for loss directly or indirectly attributable to the Company's gross negligence or

wilful default or that of any other person(s) acting for or under the control of the Company) to the extent that the law does not allow such limitation or exemption;

3.2.2 requires any person(s), Data Subject, Designated Employee or Responsible Party to assume risk or liability to the extent that the law does not allow such an assumption of risk or liability; or

3.2.3 limits or excludes warranties or obligations that are implied in this Policy by the Electronic Communications and Transactions Act (to the extent applicable), the Protection of Personal Information Act (to the extent applicable, inclusive of Regulation 4 thereto), or any other applicable laws, or any other such warranty or obligation which the Company gives under the Electronic Communications and Transactions Act, the Protection of Personal Information Act, or any other applicable law, to the extent that the law does not allow them to be limited or excluded.

## 4 SCOPE AND APPLICATION

This Policy applies to all Personal Information Processed by the Company or its Designated Employee(s) or a Responsible Party, including collection, receipt, recording, organisation, collation, storage, security, updating or modification, retrieval, alteration, consultation or use or any other method of manipulation or distribution of Personal Information.

However, as per Section 7 of the Protection of Personal Information Act, this Policy will not apply to the processinng of personal information solely for the purpose of journalistic expression, if:

- the journalist's processing of personal information is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression, and
- the journalist acts in accordance with the South African Press Code's regulations on the handling of personal information.

## 5 DATA COLLECTION COMPLIANCE

When collecting Personal Information from a Data Subject, a Responsible Party and/or Designated Employee must –

5.1 ensure that they obtain the informed consent of the Data Subject to Process the Personal Information of the concerned Data Subject, including, but not limited to, informing the Data Subject of the potential use of their Personal Information, where the Personal Information might be Processed and/or stored, as well as the notification procedures that will be used to inform the Data Subject of changes to the scope of the use of their Personal Information and/or any security breaches that might relate to their Personal Information; and

5.2 inform the Data Subject of the Data Subject's rights under the provisions of POPIA, including the Data Subject's right to -

5.2.1 object to the Processing of their Personal Information;

5.2.2 notification(s) if their Personal Information is being used for purposes other than what they consented to the Personal Informing being collected and used for;

5.2.3 establish whether the Responsible Party holds their Personal Information;

5.2.4 request that their Personal Information held by the Responsible Party be corrected or destroyed;

5.2.5 refuse the processing of their Personal Information for direct marketing purposes, such as unsolicited electronic communications;

5.2.6 lodge a complaint with the information regulator, as constituted in terms of POPIA and any regulations thereto, against the Responsible Party; and

5.2.7 institute civil proceedings against the Responsible Party.

## 6 PROCESSING PERSONAL INFORMATION

6.1 When Processing a Data Subject's Personal Information, a Responsible Party and/or Designated Employee ensure that they abided by the following conditions for the lawful Processing of Personal Information, namely -

6.1.1 **Accountability**. The Responsible Party and/or Designated Employee must ensure that the conditions set out in POPIA are complied with at the time of the determination of the purpose and means of Processing as well as during Processing itself.

6.1.2 **Purpose Specification.** The Personal Information collected from the Data Subject must be collected for a specific purpose and the Data Subject must be made aware of this purpose;

6.1.3 **Processing Limitations**. The following Processing limitations apply, namely -

6.1.3.1 the Data Subject must consent to the Processing of their Personal Information;

6.1.3.2 only the minimal amount of Personal Information needed in order to complete the Processing purpose and/or its requirements is obtained from the Data Subject;

6.1.3.3 the Data Subject must be informed of their rights as stipulated in paragraph 5.2 of this Policy and any other rights lawfully granted to the Data Subject;

6.1.3.4 all Personal Information must be collected directly from the Data Subject, except to the degree that the Data Subject consents otherwise; and

6.1.3.5 all Personal Information must be Processed lawfully and in accordance with the law.

6.1.4 **Further Processing Limitation.** The renewed consent of the Data Subject must be obtained if the Personal Information of the Data Subject must be further

Processed or if the Personal Information will be Processed for a further purpose and/or different purpose, unless the further Processing of the Data Subject's Personal Information is reasonably related to the same purpose it was initially collected for from the Data Subject;

6.1.5 **Information Quality.** Reasonable measures must be taken to ensure that the Personal Information collected from the Data Subject is complete, accurate, not misleading and is up to date. Employees are obliged to ensure that at all times they provide the Company with complete, accurate, and up to date Personal Information;

6.1.6 **Openness.** The purpose of the collection of the Data Subject's Personal Information must be transparent. The Data Subject must be reasonably made aware of their rights (as stipulated in paragraph 5.2 of this Policy) and what measures the Data Subject can take to have their Personal Information adapted or deleted, if the Data Subject in question requests this of the Responsible Party or Designated Employee;

6.1.7 **Security Safeguards.** Personal Information collected from a Data Subject must be securely kept (in accordance with the requirements stipulated in paragraph 8 of this Policy). The integrity of all Personal Information must be maintained through all technical and organisational measures and/or Processes; and

6.1.8 **Data Subject Participation.** The Data Subject has the right to request and to find out whether the Responsible Party and/or Company holds their Personal Information and a description of the Personal Information held by the Responsible Party or the Designated Employee.

## 7 ACCESS TO PERSONAL INFORMATION

Personal Information must be dealt with in the strictest confidence. No Personal Information may be disclosed by a Responsible Party or Designated Employee without first receiving the written authorisation of the Information Protection Officer, as stipulated in the Company's Information Request Manual, as amended from time to time ("**Information Request Manual**").

The Information Protection Officer is obliged to only authorise the release of and/or to disclose a Data Subject's Personal Information in accordance with the terms and conditions stipulated in the Information Request Manual and/or in accordance with any other requirements mandated by Law.

## 8 STORAGE OF PERSONAL INFORMATION

### 8.1 HARD COPIES

8.1.1 All hard copies of Personal Information must be stored at one of the Company's offices or branches. In addition to its head offices in Wright Street, Johannesburg, Caxton has additional branches in Gauteng, Limpopo, Mpumalanga, the Free State, Kwa-Zulu Natal, North West, the Eastern Cape and the Northern Cape. Furthermore, all hard copies of Personal Information must be stored in accordance with Caxton’s storage requirement and philosophy.

8.1.2 In as far as is practicable, hard copy documents are to be scanned into the Company, or an approved service provider's, internal information system and stored in accordance with paragraph 8.2.1 of this Policy. Any hard copies of the documentation must be stored in accordance with paragraph 8.1 of this Policy and must be retained for as long as the Personal Information therein is in use or, due to internal auditing requirements, for a period of five years from the date of the documents final Processing, unless otherwise agreed by the Data Subject at the date of the collection of the Data Subject's Personal Information.

### 8.2 ELECTRONIC COPIES

8.2.1 Personal Information, whether held by the Company or a Designated Employee or Responsible Party, must be stored in electronic form on the Company's or an Responsible Party's internal information system. The Company's or a Responsible Party's internal information system must have reasonable technical and organisational measures to prevent:

8.2.1.1 loss of, damage to or unauthorised destruction of any Personal Information; and

8.2.1.2 the unlawful access to or processing of Personal Information.

8.2.1.3 In order to give effect to this, the Company or approved service provider must take reasonable measures to:

8.2.1.4 identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

8.2.1.5 establish and maintain appropriate safeguards against the risks identified;

8.2.1.6 regularly verify that the safeguards are effectively implemented; and

8.2.1.7 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

8.2.2 Section 51 of the Electronic Communications Act requires that Personal Information and all documentation relating to its Processing is kept for a period of one year or for as long as such Personal Information is in use. For internal auditing requirements, this period is extended to five years from the date of the Personal Information's last Processing, unless otherwise agreed by the Data Subject at the date of the collection of such Personal Information or any subsequent date thereafter.

## 9 MAINTENANCE OF RECORDS OF PROCESSING

Responsible Parties and Designated Employees are responsible for the collection and maintenance of the records, documents and communications relating to Personal Information in accordance with paragraph 8.2.1 of this Policy.

## 10 DESTRUCTION OF PERSONAL INFORMATION

10.1 Personal Information must be destroyed or deleted after the termination of the retention period(s) outlined in paragraph 8 of this Policy and in accordance with the requirements specified in "*Documentation Destruction Guidelines*" attached to this Policy, as amended from time to time.

10.2 The Responsible Party or Designated Employee is responsible for attending to the destruction or deletion of Personal Information or any related documentation held by it on a regular basis. Personal Information must be checked before its destruction or deletion to ascertain if the information may be destroyed or deleted and whether there are any important original documents that may be returned to the Data Subject at their own cost.

10.3 After completion of the process outlined in paragraph 10.2 of this Policy, the manager of the Responsible Party or Designated Employee must authorise the destruction or deletion of the Personal Information in writing. This authorisation must be retained by the Company for a period of five years from date of receipt of the authorisation.

## 11 THIRD PARTY SERVICE PROVIDERS

11.1 The Company may disclose a Data Subject's Personal Information to a third-party service provider or Responsible Party, whose services or products the Company elects to use. Before doing so, the Company undertakes to inform the relevant Data Subjects of the movement or transfer of their Personal Information to the third-party service provider or Responsible Party and the conditions and purpose of the Processing of the Data Subjects' Personal Information with that third-party service provider or Responsible Party.

11.2 The Company must have agreements in place with any third-party service provider and/or Responsible Party warranting that the third-party service provider and/or Responsible Party contractually agrees to comply with and be bound by the terms and conditions of this Policy. The Company must ensure that in these agreements the third-party and/or Responsible Party agrees to indemnify the Company from all claims,

including claims for loss or damage (including consequential loss or damage) arising from the wilful misconduct or negligence or failure of the third-party and/or Responsible Party's behalf to abide by the terms and conditions of this Policy and/or the provisions of the Personal Information Protection Act.

11.3 The Company may also disclose a Data Subject's Personal Information to a third party where it has a duty or a right to disclose the information in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the Company's rights.

11.4 Designated Employees are responsible for ensuring that the Company abides by its obligations under paragraph 11 of this Policy.

## 12 NON-COMPLIANCE

12.1 If a Designated Employee or any other member of the Company is suspected of not abiding by the requirements outlined in this Policy or otherwise fails to comply with the terms and conditions of this Policy or any related process, then this person may be subject to an investigation and subsequent disciplinary, civil and/or criminal action.

12.2 Responsible Parties, Designated Employees and any other member of the Company are strictly liable (both directly and indirectly) for consequential loss or damage (whether pecuniary or not) to the Company's reputation or business interests or any other proprietary information or property held or owned by the Company as a result of their Processing, storage, management and security of Personal Information collected from Data Subjects on the Company's behalf or at its direction (whether as a consequence of negligent conduct or not) and may face further civil and/or criminal action thereto. The Company reserves all of its rights in this regard.

## 13 GENERAL

13.1 To ensure compliance with this Policy, periodic reviews will be conducted. These reviews may result in the modification, addition, or deletion of provision(s) of this Policy. Any

such modifications, additions, or deletions shall be deemed to have immediate effect upon their approval by the Company's management.

13.2 Any exception to this Policy must be approved by the Company's management in advance.

13.3 This Policy revokes all previous Protection of Personal Information policies of this Company and is deemed to have retrospective and immediate effect upon the date of its signature.

13.4 The signatories herewith duly authorise Helene Eloff as the Company Information Protection Officer for purposes of the Protection of Personal Information Act 4 of 2013 and the Promotion of Access to Information Act 2 of 2000. Please contact the Information Protection Officer, **Helene Eloff**, on **(+27) 82 269 6691,** or a Caxton local branch manager for any queries relating to this Policy, including the reporting of any contraventions hereto.

Signed at..... on this the..... day of .....20___

by Caxton and CTP Publishers and Printers Limited's Social and Ethics Committee.

Name: TJW Holden
Group MD

Signature: _____

Name: J Edwards

Signature: _____

Name: L Witbooi

Signature: _____

Name: PM Jenkins

Signature: _____