CDI-AMA (PTY) LTD

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE

PROTECTION OF PERSONAL INFORMATION ACT OF 2013

COMPILED WITH THE ASSISTANCE OF EMILE MYBURGH
ATTORNEYS/ADVOGADOS

CONTENTS:

Introduction	Page 2
Our Undertaking to our Clients	Page 2
Our Client's Rights	Page 4
Security Safeguards	Page 5
Security Breaches	Page 6
Clients Requesting Records	Page 7
The Correction of Personal Information	Page 8
Special Personal Information	Page 8
Processing of Personal Information of Children	Page 8
Information Officer	Page 9
Circumstances Requiring Prior Authorization	Page 10
Direct Marketing	Page 10
Transborder Information Flows	Page 11
Offences and Penalties	Page 12
Schedule of Annexures and Forms	Page 12

EMILE MYBURGH
ATTORNEYS · ADVOGADOS

A. INTRODUCTION

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

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and

2. The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for our company'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.

B. OUR UNDERTAKINGS TO OUR CLIENTS:

1. We undertake 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 our clients.

2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our clients.

3. Whenever necessary, we shall obtain consent to process personal information.

4. Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.

5. We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.

6. We shall collect personal information directly from the client whose information we require, unless:

   6.1 the information is of public record, or

6.2 the client has consented to the collection of their personal information from another source, or

6.3 the collection of the information from another source does not prejudice the client, or

6.4 the information to be collected is necessary for the maintenance of law and order or national security, or

6.5 the information is being collected to comply with a legal obligation, including an obligation to SARS, or

6.6 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

6.7 the information is required to maintain our legitimate interests; or

6.8 where requesting consent would prejudice the purpose of the collection of the information; or

6.9 where requesting consent is not reasonably practical in the circumstances.

7. We shall advise our clients of the purpose of the collection of the personal information.

8. We shall retain records of the personal information we have collected for the minimum period as required by law unless the client has furnished their consent or instructed us to retain the records for a longer period.

9. We shall destroy or delete records of the personal information (so as to deidentify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.

10. We shall restrict the processing of personal information:

10.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;

10.2 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;

10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or

10.4 where the client requests that the personal information be transmitted to another automated data processing system.

11. The further processing of personal information shall only be undertaken:

    11.1 if the requirements of paragraphs 3; 6.1; 6.4; 6.5 or 6.6 above have been met;

    11.2 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;

    11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or

    11.4 where this is required by the Information Regulator appointed in terms of POPI.

12. We undertake to ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date.

13. We undertake to retain the physical file and the electronic data related to the processing of the personal information.

14. We undertake to take special care with our client's bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.

15. Form 1 referred to in Section O below shall be sent to every client when we accept a mandate of any sort, to advise them of our duty to them in terms of POPI.

C. OUR CLIENT'S RIGHTS

1. In cases where the client's consent is required to process their personal information, this consent may be withdrawn.

2. In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.

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

4. Form 2 referred to in Section O below shall be completed by each client when we accept a mandate of any sort, to obtain the client's consent to process their personal information while we do our work for them, unless this consent has been obtained within another document signed by the client.

D. SECURITY SAFEGUARDS

[The clauses below, especially clauses 1.3 to 1.6, contain suggested measures only and must be edited and adjusted, depending on the levels of security that each company believes is reasonable and appropriate to their business and sufficient to meet the requirements of POPI. You will need the assistance of at least your IT administrator/service provider/consultant to assist with the security of your IT infrastructure.]

1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we must continue to implement the following security safeguards:

   1.1 Our business premises where records are kept must remain protected by access control, burglar alarms and armed response.

   1.2 Archived files must be stored behind locked doors and access control to these storage facilities must be implemented.

   1.3 All the user terminals on our internal computer network and our servers must be protected by passwords which must be changed on a regular basis.

   1.4 Our email infrastructure must comply with industry standard security safeguards and meet the General Data Protection Regulation (GDPR), which is standard in the European Union.

   1.5 Vulnerability assessments must be carried out on our digital infrastructure at least on an annual basis to identify weaknesses in our systems and to ensure we have adequate security in place.

   1.6 We must use an internationally recognised Firewall to protect the data on our local servers, and we must run antivirus protection at least every hour to ensure our systems are kept updated with the latest patches. The security of this system must comply with the GDPR of the European Union.

   1.7 Our staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.

   1.8 It must be a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information.

   1.9 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.

1.10 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

1.11 The digital work profiles and privileges of staff who have left our employ must be properly terminated.

1.12 The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.

2. 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.

E. SECURITY BREACHES

1. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s, unless we are no longer able to identify the client/s. This notification must take place as soon as reasonably possible.

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.

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:

3.1 by mail to the client's last known physical or postal address;

3.2 by email to the client's last known email address;

3.3 by publication on our website or in the news media; or

3.4 as directed by the Information Regulator.

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:

4.1 a description of the possible consequences of the breach;

4.2 details of the measures that we intend to take or have taken to address the breach;

4.3 the recommendation of what the client could do to mitigate the adverse effects of the breach; and

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

F. CLIENTS REQUESTING RECORDS

1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether or not we hold any personal information about that person in our records.

2. If we hold such personal information, on request, and upon payment of a fee of R500-00 plus VAT, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.

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. See form O. 4 below.

4. In certain circumstances, we will be obliged to refuse to disclose the record containing the personal information to the client. In other circumstances, we will have discretion as to whether or not to do so.

5. 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. 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.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A client is entitled to require us to correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.

2. A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.

3. Any such request must be made on the prescribed form, Form 4, referred to in Section O below [Form 2 in the Regulations].

4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

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, we 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.

6. We must notify the client who has made a request for their personal information to be corrected or deleted what action we have taken as a result of such a request.

H. SPECIAL PERSONAL INFORMATION

1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.

2. We shall not process any of this Special Personal Information without the client's consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

3. Having regard to the nature of our work, it is unlikely that we will ever have to process special personal information, but should it be necessary the guidance of the Information Officer, or their deputy/delegate, must be sought.

I. THE PROCESSING OF PERSONAL INFORMATION OF CHILDREN

1. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

J. INFORMATION OFFICER

1. Our Information Officer is Dr Ian Alastair Matheson who is our Chief Executive Officer/Managing Director or someone in a senior management position nominated and authorised by our Chief Executive Officer/Managing Director in writing. Such authorisation shall be made on Form 9 referred to in Section O below. Our Information Officer's responsibilities include:

   1.1 Ensuring compliance with POPI.

   1.2 Dealing with requests which we receive in terms of POPI.

   1.3 Working with the Information Regulator in relation to investigations.

2. Our Information Officer must designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above. Such designation shall be done by the completion of the prescribed form a copy of which is an annexure to this Compliance Manual, see Form 8 referred to in Section O below.

3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties, see Form 7 referred to in Section O below.

4. In carrying out their duties, our Information Officer must ensure that:

   4.1 this Compliance Manual is implemented;

   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;

   4.3 that this Compliance Manual is developed, monitored, maintained and made available;

   4.4 that internal measures are developed together with adequate systems to process requests for information or access to information;

   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

   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).

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

K. CIRCUMSTANCES REQUIRING PRIOR AUTHORISATION

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

   1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;

   1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;

   1.3 if we are processing information for the purposes of credit reporting (this will be important if we are making reports to assist with debtor profiling, for example, to TPN or ITC).

   1.4 if we are 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.

2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 1.1 above prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

L. DIRECT MARKETING

1. We may only carry out direct marketing (using any form of electronic communication) to clients if:

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

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

2. We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our business to them, and we may then only market BUSINESS services to them.

3. We may only carry out direct marketing (using any form of electronic communication) to other people if we have received their consent to do so.

4. We may approach a person to ask for their consent to receive direct marketing material only once, and we may not do so if they have previously refused their consent.

5. A request for consent to receive direct marketing must be made in the prescribed manner and form. The prescribed form of this request and consent is an annexure to this Compliance Manual, Form 5 referred to in Section O below.

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

M. TRANSBORDER INFORMATION FLOWS

1. We may not transfer a client's personal information to a third party in a foreign country, unless:

1.1 the client consents to this, or requests it; or

1.2 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

1.3 the transfer of the personal information is required for the performance of the contract between ourselves and the client; or

1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the client entered into between ourselves and the third party; or

1.5 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.

N. OFFENCES AND PENALTIES

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.
2. Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.
3. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.

O. SCHEDULE OF ANNEXURES AND FORMS

1. Initial letter to client.
2. Client's consent to process personal information.
3. Objection to the Processing of Personal Information (Form 1 of the Regulations).
4. Request for correction or deletion of personal information (Form 2 of the Regulations).
5. Application for consent to direct marketing (Form 4 of the Regulations)
6. Addendum to the _____ letter of appointment.
7. Information Officer's registration form.
8. Designation and delegation to Deputy Information Officer.
9. Authorisation of Information Officer.

CDI-AMA (PTY) LTD

Compiled with the assistance of EMILE MYBURGH ATTORNEYS/ADVOGADOS

Form 1: Initial letter to client

THE PROTECTION OF PERSONAL INFORMATION ACT

OUR DUTY TO YOU

Dear Client

The Protection of Personal Information Act (POPI) is now in operation and we need to comply. POPI regulates how we handle your personal information while we do our work.

POPI is intended to balance 2 competing interests, these are:

- Your constitutional right to privacy (which requires your personal information to be protected): and
- The needs of our society to have access to and to use your personal information for legitimate purposes, for example, to enable us to do our work for you.

POPI obliges us to inform you of our process, and that is the main purpose of this correspondence. If you wish to have greater insight into the way in which we implement POPI, you may ask for a copy of our company's internal POPI Compliance Manual. So, without further ado, here is what you need to know:

THE COLLECTION AND PROCESSING OF PERSONAL INFORMATION

1. We will collect the majority of your personal information from yourself. Please cooperate with us when we do so. We will also collect your personal information from any intermediary that might have referred you to us, and from public records.

2. We will be collecting your personal information to enable us to fulfil the mandate that we have been given by you. This might be the sale or purchase of a property, or the lease or hire of a property.

3. You are legally obliged to supply the information that we need to comply with the Financial Intelligence Centre Act (FICA). This information is required to combat money laundering and the financing of terrorism. Any other information that we ask for will be required to enable us to do our work. You have a choice as to whether you will supply us with this other information. Please note that if you fail to supply the information we ask for, we will not be able to do our work properly. You might also be placing yourself in breach of a contract, or the law.

4. We will be passing your personal information on to all third parties that require it for the purposes of doing their work which is related to what we are doing for you. For example, if we are working with another YOUR BUSINESS to fulfil our mandate to you, and they need your information on a deed of sale, we will share the required information with them.

5. You can rest assured that unless we are legally obliged to share your personal information, we will only share so much of your personal information as is needed by the authority that requires it, and we will only do so when it is necessary for us to do our work for you. In addition, all of our staff are bound by confidentially clauses in their letters of employment.

6. If there is an international component to the work which we are doing for you, and if we are required to share your personal information with an overseas recipient, you are entitled to ask us how your personal information will be protected in this foreign country, and we will endeavor to assist you.

7. You have the right of access to your personal information and the right to correct any errors relating to the information that we have on record. In addition, you have the right to object to us continuing to process your personal information. In this regard, please note that if you do exercise this right, we will not be able to do our work properly. In addition, this might place you in breach of a contract.

8. We are obliged by law to retain our records for a period of time after we have completed our work. During this period, your personal information will also remain protected. After this period has expired, your personal information will be destroyed in a way that de-identifies you.

THE SECURITY OF OUR SYSTEMS

9. We currently are licensed and using ESET INTERNET SECURITY which includes firewall, anti-virus, malware, ransomware and phishing protection on laptop devices.

Should you have any issues with the way in which we are processing your personal information, you are entitled to lodge a complaint with the Information Regulator, whose contact details are:

33 Hoofd Street

Forum III, 3rd Floor Braampark

P.O Box 31533

Braamfontein, Johannesburg, 2017

Complaints email: complaints.IR@justice.gov.za

General enquiries email: inforeg@justice.gov.za.

We trust however that our processing of your personal information will be handled in a way that complies with all the relevant laws and that your rights to privacy will be protected as required by law.

Kind regards

CDI-AMA PTY LTD

Form 2: Clients consent to process personal information

CONSENT TO PROCESS (USE) PERSONAL INFORMATION IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT

I/We the undersigned

_____

_____

(NAME & ID / PASSPORT NUMBER)

hereby give my/our consent for the processing (use) of our personal information by YOUR BUSINESS NAME for the purposes of carrying out the following work:

(PLEASE TICK THE APPROPRIATE BOX):

_____

_____

_____

_____

_____

Other (please specify) _____

_____

This consent specifically includes the right to work with my/our bank account details as and when required to ensure that I/we receive payments or refunds due to me/us.

This consent is furnished on condition that my/our personal information shall be used and processed in accordance with the Protection of Personal Information Act.

SIGNED AT _____(place) ON _____(date)

_____ _____

CUSTOMER CUSTOMER

Form 3: Objection to processing of personal information (Form 1 of the Regulations)

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 2]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the objection may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number / E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname/ Registered name of responsible party:	

Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f)** *(Please provide detailed reasons for the objection)*

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/designated person

Form 4: Request for correction or deletion of personal information (Form 2 of the Regulations)

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:

☐ Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐ Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and / surname data registered name of subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ( )

Contact number(s):	
Fax number/E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number/ E-mail address:	
C	**INFORMATION TO BE CORRECTED/DELETED/ DESTRUCTED/ DESTROYED**
REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. *(Please provide detailed reasons for the request)*	

Signed at ..... this ..... day of .....20……..

.....

Signature of data subject/ designated person

Form 5: Application for consent to direct marketing (Form 4 of the Regulations)

Client's names and email address and cell number:

REQUEST FOR CONSENT TO RECEIVE DIRECT MARKETING MATERIAL

SECTION 69(2) AND REGULATION 6 OF THE PROTECTION OF PERSONAL INFORMATION ACT

FORM 4 – PART A

Dear _____

We regularly send out newsflashes and other interesting information using electronic means and this could be categorized as direct marketing. We would love to have you on our mailing list, but for this to happen we need your consent.

If you would like to receive these communications, please sign off on the consent below and send it back to us.

We look forward to staying in touch.

Kind regards

CDI-AMA PTY LTD

Per:

PART B

I/We, _____(full names)

hereby **GIVE my/our CONSENT** to receive direct marketing of legal services to be marketed by means of electronic communications from CDI-AMA PTY LTD by way of (circle your choice).*

Emails SMS messages Both email and SMS

hereby **REFUSE my/our CONSENT** to receive direct Marketing of legal services to be marketed by means of electronic communications from CDI-AMA PTY LTD*

[*delete as appropriate]

Signed: Signed:

_____ _____

CLIENT CLIENT

Form 6: Addendum to the CDI-AMA PTY LTD letter of appointment

ADDENDUM TO EMPLOYMENT CONTRACT WITH CDI-AMA PTY LTD IN COMPLIANCE WITH THE PROTECTION OF PERSONAL INFORMATION ACT (POPI).

NAME OF EMPLOYEE _____

1. APPLICATION OF PROTECTION OF PERSONAL INFORMATION ACT, NO 4 OF 2013 ("the Act")

1.1. This Agreement is subject to the provisions of the Act.
1.2. "Personal Information" means in respect of the employee:
  1.2.1. 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;
  1.2.2. information relating to the education or the medical, financial, criminal or employment history;
  1.2.3. any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment;
  1.2.4. the biometric information;
  1.2.5. the personal opinions, views or preferences;
  1.2.6. correspondence sent by the employee that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  1.2.7. the views or opinions of another individual; and
  1.2.8. his or her name if it appears with other Personal Information relating to him or her or if the disclosure of the name itself would reveal information about the employee;
1.3. The Employer will handle and protect all Personal Information of the Employee in terms of the Act.
1.4. The Employer is the responsible party for purposes of the Act.
1.5. The Employer will collect Personal information only for specific, explicitly defined and lawful purposes related to a function or activity of the Employer.

1.6. The Employer shall not retain the employee's Personal Information for longer than is necessary or as required or permitted by the Act.

1.7. The Employer will take measures to prevent:
1.7.1. loss of, damage to or unauthorised destruction of Personal Information; and 1.7.2. unlawful access to or processing of Personal Information.

2. THE EMPLOYEE'S RIGHTS AND OBLIGATIONS

The Employee has the right:

2.1. to be notified that-
2.1.1. Personal Information about him, her or it is being collected; or
2.1.2. his, her or its Personal Information has been accessed or acquired by an unauthorised person;

2.2. to establish whether a responsible party holds Personal Information of that data subject and to request access to his, her or its Personal Information;

2.3. to request, where necessary, the correction, destruction or deletion of his, her or its Personal Information;

2.4. to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its Personal Information;

2.5. to object to the processing of his, her or its Personal Information at any time for purposes of direct marketing;

2.6. not to have his, her or its Personal Information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred as per the provisions of the Act;

2.7. not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its Personal Information intended to provide a profile of such;

2.8. to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal; and

2.9. to institute civil proceedings regarding the alleged interference with the protection of his, her or its Personal Information.

3. CONSENT TO GATHER INFORMATION

3.1. The Employee consents to the Employer collecting information in terms of 3.2.

3.2. The Employer will only gather information reasonably required:
3.2.1. About the employee;
3.2.2. Where processing is necessary to carry out actions for the conclusion or performance of a contract to which employee is party;

3.2.3. Where processing complies with an obligation imposed by law on the Employer;
3.2.4. Where processing protects a legitimate interest of the Employee;
3.2.5. Where processing is necessary for the proper performance of a public law duty by a public body; or
3.2.6. processing is necessary for pursuing the legitimate interests of the Employer or of a third party to whom the information is supplied.

3.3. The Employee may withdraw this information at any time (except where gathering and storing information is required by law).

Signed and dated at _____ (place) on _____ (date)

_____

EMPLOYEE

Form 7: Information Officer's registration form.

(Annexure A of the Guidance Notes issued on 1 April 2021)

ANNEXURE A

INFORMATION OFFICER'S REGISTRATION FORM

NOTE: The personal information submitted herein shall be solely used for your registration with the Information Regulator ("Regulator").

All the information submitted herein shall be used for the purpose stated above, as mandated by law. This information may be disclosed to the public. The Regulator undertakes to ensure that appropriate security control measures are implemented to protect all the information to be submitted in this document.

PART A **INFORMATION OFFICER**	
Full Name of Information Officer	
Designation	
Postal Address	
Physical Address	
Cellphone Number	
Landline Number	
Fax Number	
Direct Email Address	
General Email Address	

PART B DEPUTY INFORMATION OFFICER			
Personal details of designated or delegated Deputy Information Officer(s)	**Name**	**Name**	**Name**
	Direct Landline	**Direct Landline**	**Direct Landline**
	Cellphone Number	**Cellphone Number**	**Cellphone Number**
	Email Address	**Email Address**	**Email Address**
Postal Address			
Physical Address			
Fax Number			
General Email Address			

PART C BODY / RESPONSIBLE PARTY				
Type of Body	Public Body		Private Body	
Full Name of the Body (Registered Name)				
Trading Name				
Registration No, if any				
Postal Address				
Physical Address				
Landline Number				
Fax Number				
Email Address				
Website				

INFORMATION OFFICER

PART D

DECLARATION

SIGNED and **DATED** at_____on this the_____day of_____**2022**

PART E

THE FOLLOWING INFORMATION IS REQUIRED FOR STATISTICAL PURPOSES

Please choose a sector(s) that apply to your Body

GOVERNMENT			PUBLIC ENTITIES			PRIVATE BODY			PROFESSION		
Item	**Classification of Government**	**X**	**Item**	**Classification of a Public Entity**	**X**	**Item**	**Name of Industry Sector**	**X**	**Item**	**Type of profession**	**X**
1.	National Government		**1.**	Constitutional Entities		**1**			**1**	Legal	
2.	Provincial Government		**2.**	Schedule 2 Public Entity		**2**	Financial		**2**	Built Environment	
3.	Local Government		**3.**	Schedule 3A Public Entity		**3**	Health Facilities		**3**	Financial	
LEGISLATURE			**4.**	Schedule 3B Public Entity		**4**	Telecommunications		**4**	Medical and Allied Health Services	
National Assembly			**5.**	Schedule 3C Public Entity		**5**	Pharmaceutical		**OTHERS, Specify**		
National Council of Provinces			**OTHERS, specify**			**6**	Media and Social Media				
Gauteng Provincial Legislature						**7**	Retail/Direct Marketing				
Western Cape Provincial Legislature						**8**	Tourism		**5.**		

GOVERNMENT		PUBLIC ENTITIES	PRIVATE BODY		
Northern Cape Provincial Legislature			**9**	Transportation, Storage and Logistics	
Limpopo Provincial Legislature			**10**	Manufacturing/Production	
Northwest Provincial Legislature			**11**	Banks	
Free State Provincial Legislature			**12**	International Organizations	
Mpumalanga Provincial Legislature			**13**	Real Estate	
Eastern Cape Provincial Legislature			**OTHERS, specify**		
Kwazulu-Natal Provincial Legislature					

Form 8: Designation and delegation to Deputy Information Officer

(Annexure B of the Guidance Notes issued on 1 April 2021)

DESIGNATION AND DELEGATION OF AUTHORITY TO THE DEPUTY INFORMATION OFFICER

(*In terms of section 56 of the Protection of Personal Information Act, 2013 (POPIA) and Section 17(1) of the Promotion of Access to Information Act, 2000(PAIA)*

I, the undersigned,

_____

(Name of the Information Officer)

Please be advised that I reserve the right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties and responsibilities.

_____

Information Officer

By my signature herein below, I hereby accept the delegation and designation as the Deputy Information Officer

_____

(Name of the designate)

Date: ……..

Form 9: Authorisation of Information Officer

(Annexure C of the Guidance Notes issued on 1 April 2021)

ANNEXURE C

AUTHORISATION OF INFORMATION OFFICER

(*In terms of the Promotion of Access to Information Act, 2000)*

I, the undersigned,

DR IAN ALASTAIR MATHESON

_____

hereby authorise DR IAN ALASTAIR MATHESON as an Information Officer of CDI-AMA PTY LTD and authorise you to exercise any of the powers, duties and responsibilities conferred or imposed on me by the Protection of Personal Information Act, 2013 and the Promotion of Access to Information Act, 2000(PAIA).

Please be advised that I reserve my right to exercise any of the powers, duties and responsibilities conferred herein, as well as the right to amend and/or withdraw any of those powers, duties and responsibilities.

_____

Information Officer

By my signature herein below, I hereby accept the authorisation as an Information Officer

_____

DR IAN ALASTAIR MATHESON

Designation: **DIRECTOR**

Date: 2022-01-01