

CLAMAN PTY LIMITED

COMPLIANCE MANUAL

FOR THE IMPLEMENTATION OF THE PROTECTION OF PERSONAL INFORMATION ACT OF 2013

CONTENTS:

- A1. Introduction
- A2. Categories of personal information collected
- B. Undertaking in terms of POPI Act 4 of 2013
- C. Our Parties' (including Employees') Rights
- D. Security Safeguards
- E. Security Breaches
- F. Parties, including Employees, Requesting Records
- G. The Correction of Personal Information
- H. Special Personal Information
- I. Processing of Personal Information of Children
- J. Information Officer
- K. Circumstances Requiring Prior Authorization
- L. Direct Marketing / Circulation of Newsletters and Advisories
- M. Transborder Information Flows
- N. Offences and Penalties
- O. Schedule of Annexures and Forms

A1. Introduction

About Claman Pty Limited ("Company"):

The Company was founded in 1996, by Clarissa Heyman, and started trading wef 1 July 1996 as the exclusive agent in South Africa for Robertet (France) who are one of the largest fragrance and flavourant producers in the world.

A small staff complement is employed to cover the warehousing, distribution, marketing and administration activities of the Company.

Purpose of POPI Act 4 2013

The Protection of Personal Information Act (or POPI Act) is South Africa's equivalent of the EU GDPR. It sets some conditions for responsible parties (called controllers in other jurisdictions) to lawfully process the personal information of data subjects (both natural and juristic persons).

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.

Company Compliance Manual

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.

A2. Categories of personal Information collected by Company

Company may possess records relating to Clients, Suppliers/ Vendors, Service Providers, Sub-Contractors and Employees (collectively referred to as "the Parties"):					
Data Subject	Information Processed	Who processes the information at Company	Purpose for personal information processing	How personal data processed	Risk Assessment – negative impact on subject of misuse of data. ** see below

Personal information - partly publicly and partly not publicly available					
Clients – Natural and Juristic Persons	Names, contact details, postal address, date of birth, ID number, Tax & bank related, nationality, gender	All Employees, Delivery Sub-Contractors	Communication between staff, used by Staff in sale of goods and arranging delivery by Sub-Contractors for the effective management of the sales	1.General contact list 2. Invoicing, accounting, banking 3. Credit Applications and contractual records	1 and 2: low risk 3: medium risk
Employees	Gender, Pregnancy, Marital Status, Ethnicity, Age, Language, Education information, Bank and Tax details (for salary), Employment History, ID number, Physical and Postal address, Contact details, Criminal behaviour, Well-being, COVID related info	Managing director, Administration & HR Manager	Required in the normal course of employment and as allowed in terms of labour law. Effective management of the Company.	Records maintained by Administration & HR Manager	Medium to High Risk
Suppliers / Vendors, Clients and Sub-Contractors entering the Company's business premises	Names of contact persons, phone contact details, Vehicle Registration Numbers, signatures, COVID related info.	Receptionist	Maintain security of the Company's business premises	Record of entries retained in Receptionists' office	Low risk
Generally publicly available information					
Service Providers &	Names of contact persons; Name	All Employees	For effective management	Filed in Company's offices along	Low risk

Sub-Contractors to Company	of Legal Entity, Physical and Postal address and contact details, Registration Number, Tax & bank related, authorised signatories, COVID related info		of the Company	with accounting records.	
Suppliers/ Vendors to Company	Names of contact persons; Name of Legal Entity, Physical and Postal addresses, contact details, Registration Number, Tax & bank related, founding documents, COVID related info	All Employees	For effective management of the Company	Filed in Company's offices along with accounting records.	Low risk

****Potential risk to personal data:** Loss of privacy, Identify theft, unauthorised access or purchase by third party e.g. for direct marketing, by hackers, for spamming, malicious online activity.

B. UNDERTAKING IN TERMS OF POPI ACT 4 OF 2013:

1. We, the Directors and Employees of the Company, undertake to follow the POPI Act at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of the Parties and at the same time to enable the smooth running of the Company's business activities.

The records of Employees' personal details retained by the Company are kept in a locked cabinet in a locked office. The requisite back-up, safety and security procedures including anti-virus and malware protection are available on the computers processing this information and using this data.

The same care will be taken to safeguard the integrity, accuracy and use of the personal information collected from Clients, Suppliers/ Vendors, Service Providers and Sub-Contractors.

2. We undertake to process information from the Parties, only for the purpose for which it is intended, to enable the Company and Employees to conduct the business activities, as agreed with its Directors and Employees and confirmed in this Compliance Manual.

3. Whenever necessary, Company shall obtain consent to process personal information where this has not been obtained.
7. We shall advise all Parties of the purpose for 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 and for as long as it is necessary to fulfill legal or contractual obligations to the Parties, and for historical and statistical purposes.
9. We shall destroy or delete records of the personal information (so as to de-identify the parties) as soon as the requirements of point 8 no longer pertain.
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 Parties' bank account details, and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the Parties' specific consent.
15. Form 1 (Initial letter to Clients referred to in point 1 of Section O below) shall be sent to every Client whenever considered necessary.
16. Service Providers and Sub-Contractors to the Company in possession of personal information of Clients in the normal course of business will be contractually required by the Company to confirm to the data protection requirements of POPI Act 4 of 2013.

C. OUR CLIENTS' AND EMPLOYEES' RIGHTS

1. In cases where the Clients' and Employees' 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 the Company's legitimate interests, the Client / Employee 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. Form 1 of the Regulations referred to below in point 2 of section O.
4. Form 3 referred to in point 3 Section O below shall be completed by each Client or Employee to request the correction or deletion of personal information.

D. SECURITY SAFEGUARDS

1. Care will be taken to ensure that personal records of Clients and Employees, whether manual or electronic are protected from unauthorized access, loss or damage.
2. All Employees involved in the use and processing of personal information of Clients, Suppliers/ Vendors, Service Providers and Sub-Contractors entering the Company's business

premises, are instructed on the minimum requirements for protection of personal records from unauthorized use, loss, or damage.

3. Contracts with Service Providers and Sub-Contractors will specify the limits of use of all Parties' personal data as well the requirement that they are protected from unauthorized access, use, loss of damage.
4. These security safeguards should be verified from time to time to ensure effective implementation, and must be updated in response to new risks or deficiencies.

E. SECURITY BREACHES

1. Where there has been a breach of personal data which has been accessed or acquired by an unauthorized person, or has not been used for the purposes intended, and has had a significant negative impact on the data subject affected, the data subject and the Information Regulator must be informed as soon as reasonably possible by the most appropriate means available.
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 relevant Party(ies) be delayed.
3. Notification to Parties must give sufficient information for Parties to protect themselves against the potential consequences of the security breach, and given details of the measures to be taken to address the breach, mitigate the adverse effects of the breach and the identity of the person who may have accessed the personal information.

F. REQUESTING OF 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 (to be decided) we shall provide the person with the record.
3. A Party 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 3 of the Regulations in section O, point 3 below.

G. THE CORRECTION OF PERSONAL INFORMATION

1. A Party 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 data subject is also entitled to require us to destroy or delete records of personal information about the subject that is no longer correct or relevant.

3. Any such request must be supplied to the Information Officer or Deputy in writing by email, or hard copy or be made on the prescribed form, Form 3, referred to in point 3 Section O below [It is Form 2 in the Regulations].
4. Upon receipt of such a lawful request, the Company must comply as soon as reasonably practicable.
6. We must notify the data subject 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 Party'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 the Company's business activities, it is unlikely that the Company 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

This is not likely to occur in our Company, but in the event that it does:

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 **Clarissa Heyman** who is Managing Director (or alternatively from time to time someone in a senior management position nominated and authorised by our Managing Director in writing). Such authorisation shall be made on Form 7 referred to in point 7 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 6 referred to in point 6 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 5 referred to in point 5 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 Compliance 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

This is not likely to occur at the Company, but in event of it doing so:

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 for Parties (account numbers, file numbers or other numbers or codes allocated to Parties for the purposes of identifying them in the business of our Company) 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.
 - 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. NEWSLETTERS, NOTICES AND ADVISORIES AND DIRECT MARKETING TO PARTIES AND NON PARTIES

1. We may circulate newsletter, notices, and advisories to Parties using their personal information, if we have obtained their personal information in the context of the Company providing services relevant to Parties.

However, we may only carry out direct marketing using any form of electronic communication to Parties if:

- 1.1 they were given an opportunity to object to receiving direct marketing material by electronic communication; and
 - 1.2 they did not object then or at any time after receiving any such communications from us.
 - 1.3 We, and our agents, may only carry out direct marketing of the Company's activities (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 has not been included as an annexure to this Compliance Manual as it is not envisaged that the Company will conduct any direct marketing, or similar, activities.
6. All direct marketing communications must disclose our identity and contain an address or other contact details to which the Parties may send a request that the communications cease.

M. TRANS BORDER INFORMATION FLOWS

Not likely to occur at the Company, but in event of it doing so:

1. We may not transfer a Party's personal information to a third party in a foreign country, unless:
 - 1.1 the Party 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 the Company and the Party; or
- 1.4 the transfer is necessary for the conclusion or performance of a contract for the benefit of the Party entered into between the Company and the third party; or
- 1.5 the transfer of the personal information is for the benefit of the Party and it is not reasonably possible to obtain their consent and that if it were possible the Party 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 Parties' personal information in the same way as if it were our own.

O. SCHEDULE OF ANNEXURES AND FORMS

1. Initial letter to Clients.
2. Objection to the Processing of Personal Information (Form 1 of the Regulations).
3. Request for correction or deletion of Personal Information (Form 2 of the Regulations).
4. Addendum to Employees' Employment Contract.
5. Information Officer's registration form.
6. Designation and delegation to Deputy Information Officer.
7. Authorisation of Information Officer.

Form 1: Initial letter to Clients

DOCUMENT TO BE PLACED ON CLAMAN PTY LTD LETTERHEAD

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 co-operate with us when we do so. We will also collect your personal information from public records.
2. We will be collecting your personal information to enable us to fulfil the mandate that we have as a supplier to your organisation.
3. 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 processing clients' personal information are bound by confidentiality and proper use requirements confirmed to them.
4. 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 may not be able to do our work for you properly. In addition, this might place you in breach of a contract.
5. We are obliged by law to retain our records for a period of time after we have completed our obligations to you as a supplier. 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

6. The hard copy records of your personal details retained by our Company are kept in a locked cabinet in a locked office. The requisite back-up, safety and security procedures including anti-virus and malware protection are available on the computers processing this information at our Company's premises.

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: infoereg@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

Managing Director

Claman Pty Limited

Form 2: 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:	
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:	
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 3: 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 / 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	INFORMATION TO BE CORRECTED/DELETED/ DESTROYED/ DESTROYED

Form 4: Addendum to the CLAMAN PTY LIMITED letter of appointment

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

NAME OF EMPLOYEE _____

1. The Employee hereby acknowledges receiving training on the Company's POPI Compliance Manual.
2. The employee hereby undertakes:
 - 2.1 to comply with the terms of the POPI Compliance Manual; and
 - 2.2 to maintain the confidentiality of all our Clients and colleagues personal information and affairs.
 - 2.3 to notify the Managing Director of the Company immediately where there are reasonable grounds to believe that the personal information of a Client or a colleague has been accessed or acquired by any unauthorised person.
3. The Employee hereby gives their consent for their personal information held by the Employer to be processed for the purposes of their employment with the Employer, in accordance with the provisions of POPI and any applicable labour and taxation laws.

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

EMPLOYEE

Form 5: 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	(SOUTH AFRICA)		
Designation			
Postal Address	Ensuring protection of your personal information and effective access to information		
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)	(SOUTH AFRICA)			
Trading Name				
Registration No, if any	Ensuring protection of your personal information and effective access to information			
Postal Address				
Physical Address				
Landline Number				
Fax Number				
Email Address				
Website				

PART D
DECLARATION

I declare that the information contained herein is true, correct and accurate.

*Ensuring protection of your personal information
and effective access to information*

SIGNED and DATED at _____ on this the _____ day of

_____ **202**__

INFORMATION OFFICER

**PART E – INFORMATION
REQUIRED FOR STATISTICAL
PURPOSES (See separate
sheet)**

**Form 6: 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)

hereby designate.....

(name of the person being designated) as a Deputy Information Officer of

.....(name of the body or

Furthermore, I hereby delegate to you the following powers, duties and responsibilities, as
conferred or imposed on me by POPIA and PAIA

*Ensuring protection of your personal information
and effective access to information*

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 7: 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,

(Name of the Information Officer)

hereby authorise.....(**name of the person being designated**) as an Information Officer of(**name of the body or responsible party**) 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

(Name of the person authorised)

Designation: _____

Date: