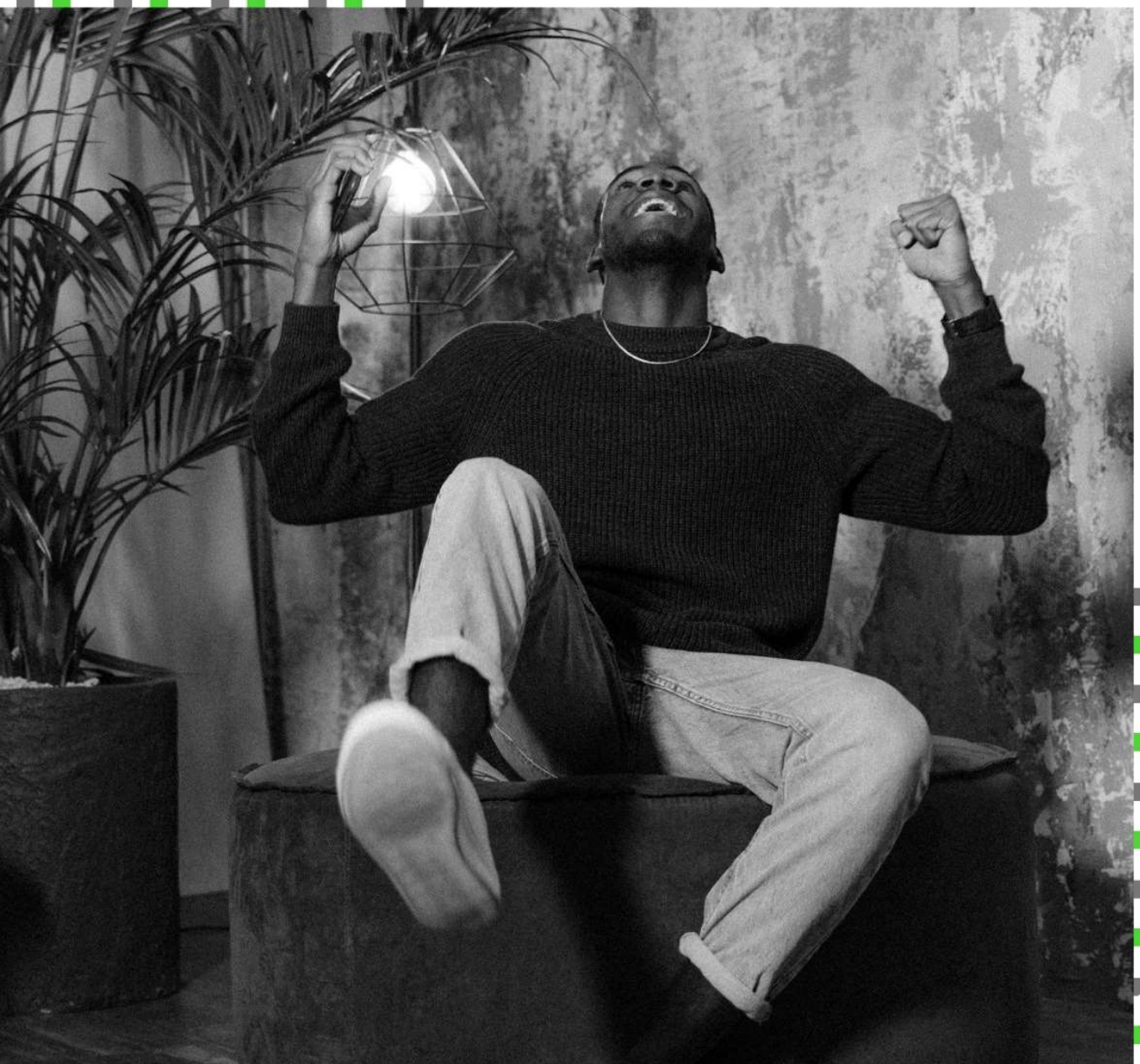
innovance

advancing innovation

Compliance Manual for the Implementation of the Protection of Personal Information Act of 2013



Version 20231010

Table of Contents

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.

Our Undertaking 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 We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised. Please refer to Form 1 in Annexure F for completion in lodging an objection.
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 de-identify 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. Letter in Annexure A 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.

Our Clients 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 in Annexure B 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.

Security Safeguards

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, burglar alarms and armed response must remain active.
   - 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.
   - 1.5. We must use an internationally recognised Firewall to protect the data on our local computers and servers, and we must have active antivirus on all devices accessing and storing data.
   - 1.6. Our staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.
   - 1.7. 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.
   - 1.8. Employment contracts for staff whose duty it is to process a client's personal information, must include an obligation on the staff member
     - 1.8.1. to maintain the Company's security measures, and
     - 1.8.2. 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. Refer to Annexure C for an example of the relevant addendum/clause to be used in these contracts.

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

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

1.11. 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.

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.

Clients Requesting Records

1. On production of proof of identity, any person is entitled to request that we confirm, free of charge, whether we hold any personal information about that person in our records.
2. Unless we are bound to by law, contractually or without express consent of the data subject, no personal information will be disclosed or shared.
3. A client or data subject are encouraged to maintain their personal details and advise us in writing of any changes to their personal information. See Annexure D – Form 2 for completion and submission.

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 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.

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 2 in Annexure D.
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.

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 required for us to have to process special personal information.
4. We will not collect, process or store excessive information or special information. Should the extent of special information that is collected, processed and stored be in question, guidance will first be obtained from the information officer.

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.

Information Officer

1. Our Information Officer is **Kylie Massey** who is our Managing Member. Our information officer may appoint a senior manager to fulfil part, or all their obligations as set out below. The authorisation registration certificate is provided in Annexure E. 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 when necessary and the certificate in Annexure E will be amended accordingly.
3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties. The registration certificate in Annexure E will be amended accordingly.
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.

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 (for example, 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.

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.

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.

Schedule of Annexures and Forms

1. Annexure A: Initial letter to client.
2. Annexure B: Client's consent to process personal information.
3. Annexure C: POPIA Contract of Employment Clauses.
4. Annexure D: POPIA Form 2 Correction or Deletion of Personal Information
5. Annexure E: Information Regulator Registration Certificate
6. Annexure F: POPIA Form 1 Objection to the Processing of Personal Information
7. Annexure G: POPIA Form 3 Outcome of Request and Fees Payable
8. Annexure H: POPIA Form 4 Internal Appeal Form

Annexure A

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:

1. Your constitutional right to privacy (which requires your person al information to be protected): and
2. 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 click on this LINK to read our company's internal POPI Compliance Framework. 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 an intermediary that you might have used, for example, an employment agency or an employer.
2. We will be collecting your personal information to enable us to fulfil the mandate that we have been given. These mandates may include, but are not necessarily limited to: employment services, payroll and related services, bookkeeping and related services, human resource consulting services.
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. In addition, this might place you in breach of contract.

4. We will be passing your personal information on to all the necessary authorities that require it for the purposes of doing their work which is related to what we are doing for you. For example, SARS, Department of Labour, Bargaining Council's and Unions.
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. 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 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

1. On the issue of the transfer of personal information overseas, kindly note that our email server runs on Outlook 365 and the data is therefore stored in the "cloud", wherever that might be. This email infrastructure does however comply with rigorous security safeguards.
2. We are also using an internationally recognised Firewall to protect the data on our local servers, and antivirus is active on all devices which have access to data or our systems.

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.

Annexure B

Consent to Process (Use) Personal Information in Terms of the Protection of Personal Information ACT

I/We the undersigned

_____,

hereby give my/our consent for the processing (use) of our personal information by INNOVANCE OUTSOURCED BUSINESS SERVICES CC

for the purposes of carrying out the following:

(PLEASE TICK THE APPROPRIATE BOX):

☐ The Preparation of a Curriculum Vitea

☐ Application for Employment

☐ Payroll processing

☐ SARS Returns and Reporting

☐ Preparation of Management Accounts

☐ Credit Checks

☐ Criminal Checks

□ Human Resource Contracts and Hearings

□ Department of Labour Returns and Reporting

□ Other (please specify) _____

Candidates applying for a position that we advertise, on behalf of our Clients, consent to us processing their Personal Information through a third-party data provider where necessary. Only such information that is absolutely necessary will be shared with the third-party for the express purpose of obtaining credit reports. You agree that these credit reports may be shared with our Client and only in the event that the Client would like to make an offer of employment. You acknowledge that this process and the information we obtain may remove you from the list of candidates we put forward to our Client. We will share any basic information with you, but should you wish to have a copy of the detailed reports, you would be required to re-imburse us for the cost of the report. Should you be placed through us with one of our Clients, we will waive the fee and provide the full report to you at our cost.

This consent specifically includes the right to obtain and utilize my bank account details.

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)

_____ _____

(Name & Surname) (Signature)

Annexure C

Employee Contractual Confidentiality Clauses

1. The Employee acknowledges that he/she may, during the course of his/her employment with the Employer, gain access to, become acquainted with or come into the possession of private, sensitive and confidential information of the Employer, whether in oral, written, electronic or another form, which includes but is not limited to information relating to the Employer's business, trade secrets, financial methods, 'know how', research and development, strategies, financial position, financing techniques, financial projections, profit margin information, corporate information, transactions, current and/or future business plans and models, software, policies and procedures, marketing methods, client lists, client details, client matter information, information databases, incentive and reward schemes, remuneration structures, personnel information, associated entities, business processes and systems, suppliers and service providers, strategic partners, business associates, security information, training materials, personal information as contemplated in terms of POPIA relating to the Employer, other employees, clients and any other third parties in the possession of the Employer, as well as other information which relates to the Employer and is not in the public domain and could reasonably be assumed to be private and confidential information of the Employer regardless of whether such information is designated as 'confidential information' at the time of its disclosure (hereinafter referred to as "Confidential Information").

2. The Employee undertakes for the duration of this employment agreement as well as after termination thereof, except as specifically required for the execution of his/her tasks and duties, not to directly or indirectly, utilize, disclose, allow access to or make public to any unauthorized person or third party for any reason whatsoever the Confidential Information or derive any economic value, benefit or profit from the use of such Confidential Information, save as expressly authorized by the Employer, or required by any applicable law or court to be disclosed, and

then only to be disclosed to the extent required by such law and subject where possible, to a similar undertaking of confidentiality as contained in this clause.

3. Without derogating from the generality of the exceptions stipulated in clause [2], it is hereby recorded for the avoidance of any doubt, that the Confidential Information shall not include –

3.1. information which was known to the Employee prior to its receipt from the Employer;

3.2. information which is or lawfully becomes generally available to the public;

3.3. information which is lawfully acquired from third parties who have a right to disclose such information;

3.4. information which by mutual agreement is released from confidential status; and

3.5. information which is required to be disclosed in response to a valid order of court or other governmental agency or if disclosure is otherwise required by law, and the Employee shall provide the Employer with prompt written notice if such disclosure is required, and shall limit the disclosure to the minimum necessary to comply with the law.

4. The onus of proof shall at all times rest on the Employee to establish that any information falls within the exclusions referred to in clause [3] above.

5. The Employee hereby indemnifies and holds harmless the Employer from and against all claims, losses, damages, liabilities, costs and expenses (including without limitation reasonable expenses of investigation and reasonable legal fees on an attorney and client scale, and pre- and post-judgement interest and penalties) arising from any breach of this clause [5] by the Employee.

Annexure D

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

_____
_____
_____
_____
(Address)

E-mail address: _____

Fax number: _____

*Mark with an **"X"***

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request is made *(if applicable):*				
Identity Number				
Postal Address				

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			

PARTICULARS OF RECORD REQUESTED

Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (*If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)*

Description of record or relevant part of the record:	
Reference number, if available	
Any further particulars of record	

TYPE OF RECORD
*(Mark the applicable box with an "**X**")*

Record is in written or printed form	
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Record consists of recorded words or information which can be reproduced in sound	
Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "**X**")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) A request fee must be paid before the request will be considered. *b) You will be notified of the amount of the access fee to be paid.* *c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	**Facsimile**	**Electronic communication** ***(Please specify)***

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Requester / person on whose behalf request is made

---

FOR OFFICIAL USE

Reference number:	
Request received by: (State Rank, Name And Surname of Information Officer)	
Date received:	
Access fees:	
Deposit (if any):	

_____

Signature of Information Officer

Annexure E

INFORMATION REGULATOR (SOUTH AFRICA)

Ensuring protection of your personal information and effective access to information

REGISTRATION CERTIFICATE

Registration Number: 0002548/2023-2024-IRRT/PR

This is to certify that **Kylie Massey** has been registered as the **Information Officer** with the Information Regulator by **InnoVance Outsourced Business Services**, in terms of section 55(2) of the Protection of Personal Information Act 4 of 2013 on the **14 March 2023**.

Chief Executive Officer
INFORMATION REGULATOR

NB: Please note that it is your responsibility to ensure that the particulars of an Information Officer and/or Deputy Information Officer(s) are correct and updated on an annual basis or as when it becomes necessary.

Annexure F

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, 2017

[Regulation 2(1)]

Note:

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

Reference Number….

A	**DETAILS OF DATA SUBJECT**
Name and surname of data subject:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
B	**DETAILS OF RESPONSIBLE PARTY**
Name and surname of responsible party*(if the responsible party is a natural)*:	
Residential, postal or business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	

Name of public or private body*(if the responsible party is not a natural person)*:	
Business address:	
	Code ( )
Contact number(s):	
Fax number:	
E-mail address:	
C	**REASONS FOR OBJECTION** *(Please provide detailed reasons for the objection)*

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

.....
Signature of data subject (applicant)

Annexure G

FORM 3
OUTCOME OF REQUEST AND OF FEES PAYABLE
[Regulation 8]

Note:

1. *If your request is granted the—*
   (a) *amount of the deposit, (if any), is payable before your request is processed; and*
   (b) *requested record/portion of the record will only be released once proof of full payment is received.*
2. *Please use the reference number hereunder in all future correspondence.*

Reference number: _____

TO: _____
_____
_____
_____

Your request dated _____, refers.

1. You requested:

Personal inspection of information at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)* is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you. If you then require any form of reproduction of the information, you will be liable for the fees prescribed in Annexure B.	

OR

2. You requested:

Printed copies of the information *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of information on flash drive *(including virtual images and soundtracks)*	
Copy of information on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

3. To be submitted:

Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language: *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

Kindly note that your request has been:

☐ Approved

☐ Denied, for the following reasons:

4. Fees payable with regards to your request:

Item	Cost per A4-size page or part thereof/item	Number of pages/items	Total
Photocopy			
Printed copy			
For a copy in a computer-readable form on: (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60.00		
For a transcription of visual images per A4-size page	Service to be outsourced. Will depend on the quotation of the service provider		
Copy of visual images			
Transcription of an audio record, per A4-size	R24.00		
Copy of an audio record (i) Flash drive • To be provided by requestor (ii) Compact disc • If provided by requestor • If provided to the requestor	 R40.00 R40.00 R60. 00		
Postage, e-mail or any other electronic transfer:	Actual costs		
TOTAL:			

5. Deposit payable (if search exceeds six hours):

☐ Yes ☐ No

Hours of search		Amount of deposit *(calculated on one third of total amount per request)*	

The amount must be paid into the following Bank account:
Name of Bank: _____
Name of account holder: _____
Type of account: _____
Account number: _____
Branch Code: _____
Reference Nr: _____
Submit proof of payment to: _____

Signed at _____ this _____ day of _____ 20 _____

_____
Information officer

Annexure H

INTERNAL APPEAL FORM

FORM 4

[Regulation 9]

Reference Number: **……..**

PARTICULARS OF PUBLIC BODY				
Name of Public Body				
Name and Surname of Information Officer:				
PARTICULARS OF COMPLAINANT WHO LODGES THE INTERNAL APPEAL				
Full Names				
Identity Number				
Postal Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				
Is the internal appeal lodged on behalf of another person?	Yes	☐	No	☐
If answer is "yes", capacity in which an internal appeal on behalf of another person is lodged: *(Proof of the capacity in which appeal is lodged, if applicable, must be attached.)*				
PARTICULARS OF PERSON ON WHOSE BEHALF THE INTERNAL APPEAL IS LODGED ***(If lodged by a third party)***				
Full Names				
Identity Number				
Postal Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
E-Mail Address				

DECISION AGAINST WHICH THE INTERNAL APPEAL IS LODGED *(mark the appropriate box with an "X")*	
Refusal of request for access	
Decision regarding fees prescribed in terms of section 22 of the Act	
Decision regarding the extension of the period within which the request must be dealt with in terms of section 26(1) of the Act	
Decision in terms of section 29(3) of the Act to refuse access in the form requested by the requester	
Decision to grant request for access	

GROUNDS FOR APPEAL *(If the provided space is inadequate, please continue on a separate page and attach it to this form. all the additional pages must be signed)*	
State the grounds on which the internal appeal is based:	
State any other information that may be relevant in considering the appeal:	

You will be notified in writing of the decision on your internal appeal. Please indicate your preferred manner of notification:

Postal address	Facsimile	Electronic communication *(Please specify)*

Signed at _____ this _____ day of _____ 20 _____

_____

Signature of Appellant/Third party

FOR OFFICIAL USE

OFFICIAL RECORD OF INTERNAL APPEAL

Appeal received by: *(state rank, name and surname of Information Officer)*				
Date received:				
Appeal accompanied by the reasons for the information officer's decision and, where applicable, the particulars of any third party to whom or which the record relates, submitted by the information officer:		Yes ☐ No ☐		
OUTCOME OF APPEAL				
Refusal of request for access. Confirmed?	Yes No	☐ ☐	New decision *(if not confirmed)*	
Fees (Sec 22). Confirmed?	Yes No	☐ ☐	New decision *(if not confirmed)*	
Extension (Sec 26(1)). Confirmed?	Yes No	☐ ☐	New decision *(if not confirmed)*	
Access (Sec 29(3)). Confirmed?	Yes No	☐ ☐	New decision *(if not confirmed)*	
Request for access granted. Confirmed?	Yes No	☐ ☐	New decision *(if not confirmed)*	

Signed at _____ this _____ day of _____ 20 _____

_____

Relevant Authority

Contact us:

011 465 2558

083 442 0939

kylie@innovance.co.za

www.innovance.co.za