PAIA MANUAL

of

XSCAPE4U PTY LTD

(Registration no: 2020/572045/07

This Manual is prepared in terms of Section 51 of the Promotion of Access to Information Act No 2 of 2000 (“PAIA”) as amended by the Protection of Personal Information Act, No 4 of 2013 (“POPIA”)

TABLE OF CONTENTS

1. DEFINITIONS

"Xscape4u", "we", "us" and "our"	means Xscape4u Pty Ltd (registration number 2020/572045/07),
"Data Subject"	means the person to whom the personal information relates.
"Manual"	means this Xscape4u PAIA manual, together with all appendices hereto.
"PAIA"	means the of Promotion of Access to Information Act, No 2 of 2000.
"POPIA"	means the Protection of Personal Information Act, No 4 of 2013.
"Processing"	means any operation or activity, whether by automatic means, concerning personal information including collection, receipt, storage, alteration, erasure, as further defined in POPIA.
"Record"	means any recorded information, regardless of form or medium which includes writing, label, marking, hardware, software, book, image (as further defined in POPIA).
"Regulator"	means the Information Regulator as defined in POPIA and established in terms of section 39 of POPIA.
"Requestor"	means any private body, any person, including a public body or official thereof, making a Request for Access to a Record of that private body, or a person acting on behalf of the aforesaid person.
"Request for Access"	means as promulgated in section 1 of PAIA, in relation to a private body, means a Request for Access to a record of a private body in terms of section 50.

2. INTRODUCTION TO PAIA AND POPIA

PAIA:

The Promotion of Access to Information Act, 2000 ("PAIA") commenced on 9 March 2001, which among other things:

- seeks to give effect to a person's Constitutional right of access to information (subject to certain limitations) and sets out the procedural process to follow to exercise or protect this right.
- sets out the obligation of private bodies to compile a PAIA Manual.

Thus, where a person is desirous of obtaining information from Xscape4u in terms of PAIA, such request must be made in the format as prescribed under this Xscape4u PAIA Manual, and following receipt of the request, Xscape4u must decide if it is able to provide the requested information to the Requester in accordance with the provisions of PAIA.

POPIA:

The Protection of Personal Information Act, 2013 ("POPIA") commenced on 1 July 2020 and gives effect to:

- a person's right to privacy, including the right to data privacy, and in accordance with this objective, describes and prescribes a series of conditions which must be met when personal information is processed, which conditions establish the minimum requirements for the Processing of personal information.
- amends certain provisions of PAIA, balancing the need for access to information against the need to ensure the protection of personal information.

This PAIA Manual is compiled in accordance with section 51 of PAIA as amended by POPIA.

3. PURPOSE OF THE PAIA MANUAL

The purpose of this Manual:

- For purposes of PAIA: details the procedure that a Requester is to follow making a Request for Access, and the way a Request for Access will be facilitated by Xscape4u.

- For purposes of POPIA: details the purpose for which personal information may be processed; a description of the categories of Data Subjects for whom Xscape4u processes personal information, as well as the categories of personal information relating to such Data Subjects and the recipients to whom personal information may be supplied.

4. THE INFORMATION REGULATOR'S PAIA GUIDE

The Regulator has compiled an official PAIA Guide which is user-friendly and accessible to assist in understanding how to exercise any right contemplated in PAIA or POPIA.

Should you have any queries, or require a copy of the Guide, contact the Regulator directly:

Address:	The Information Regulator (South Africa) JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001 P.O. Box 31533, Braamfontein, Johannesburg, 2017
Telephone Number:	+27 (0)10 023 5207
E-mail Address:	General enquiries: enquiries@inforegulator.org.za
Website	https://inforegulator.org.za/

5. COMPANY OVERVIEW

Xscape4u is a local tour operator, offering handpicked holiday packages to various destinations within Southern African & surrounds, providing an end-to-end customer service to all customers within South Africa & abroad.

6. XSCAPE4U - CONTACT DETAILS

Chief Executive Officer	Samantha Mitchell
Physical Address	23 Morris Street, Woodmead Exchange Building, Woodmead
Postal Address	P O Box 787214, Sandton, 2146
Telephone Number/Head Office **Mobile Number**	+27 (0) 10 3008704 +27 (0) 82 6572274
Email Address	info@xscape4u.com

7. DESCRIPTION OF SUBJECTS AND CATEGORIES OF RECORDS

Xscape4u maintains Records on the categories and subject matters listed below.

Recording a subject matter or category does not imply that a Request for Access to such Record(s) will be granted. All Requests for Access will be evaluated on a case-by-case basis in accordance with the provisions of PAIA.

Please note that many of the Records held by Xscape4u are those of third parties, such as clients and employees, and we take the protection of third-party confidential information seriously.

Requests for Access to these Records will be carefully considered.

Subjects of Records	Categories of Records
Statutory Company Information	○ Incorporation documents ○ Memorandum of Incorporation ○ Minute books, Resolutions ○ Records of all subsidiary companies ○ Registers of directors and officers ○ Share registers and other statutory registers ○ Statutory returns to relevant authorities ○ Statutory Records ○ Records relating to appointment of directors, auditors, company secretary, public officer ,and other officers.
Financial and Accounting Records	○ Annual Financial Statements ○ Accounting Records (inclusive of books of account) ○ Administrative Records ○ Banking Records ○ Internal and external audit reports ○ Rental agreements ○ Invoices ○ Supporting schedules and documentation to books of account ○ Lease agreements ○ Asset registers ○ Sale Agreements ○ Intellectual Property records
Tax Records	○ Customs and Excise Records ○ Income tax returns and other documentation ○ PAYE Records ○ Regional services council Records ○ Skills Development Levies Records ○ Stamp Duties Records ○ UIF and Workmen's compensation ○ Value Added Tax Records
Legal Records	○ Documentation pertaining to litigation or arbitration ○ General agreements and contracts ○ Licenses, permits and authorizations

Customer Records and Credit Services	○ Customer contracts ○ Credit application forms ○ Customer Records ○ Debtors with collection agents ○ Records of customer details and payment performance listed with credit bureaus ○ Sales Records ○ Terms and conditions of sale ○ Transaction Records
Supplier /Third Party Records	○ Code of Conduct ○ Supplier contracts ○ Terms and conditions for dealing with suppliers ○ Transactional Records and supporting information

8. INFORMATION RELATED TO PERSONAL INFORMATION

Introduction

The Protection of Personal Information Act, 4 of 2013 (POPIA), regulates and controls the Processing, including the collection, use, and transfer of personal information relating to identifiable, living, natural persons and juristic persons.

Personal information as defined in terms of POPIA includes but is not limited to, information as follows: Name, address, contact details, date of birth, place of birth, identity number, colour, ethnic or social origin, religion, identifying number, passport number, bank details, tax number, financial information, biometric information, personal opinions or views of a person, criminal history, membership of a trade union, images by way of CCTV.

In terms of POPIA, a person (Responsible Party) has a legal duty to collect, use, transfer and destroy (process) another's (Data Subject) personal information (Personal Information) in a lawful, legitimate, and responsible manner and in accordance with the provisions and 8 Processing conditions set out under POPIA.

How to request your personal information under POPIA

Requests for personal information under POPIA must be made in accordance with the provisions of PAIA which process is outlined below in Section 11.

If we provide you with your personal information, you have the right to request the correction, deletion, or destruction ("rectification") of your personal information, on the prescribed form (APPENDIX D hereto). You may also object to the Processing of your personal information on the prescribed form (APPENDIX C hereto).

Purpose of Processing personal information

POPIA provides that personal information may only be processed lawfully and in a reasonable manner that does not infringe upon the Data Subject's privacy.

The type of personal information that we process will depend on the purpose for which it is collected. We will disclose the reason the personal information is being collected and will process the personal information for that purpose only.

Information is required by Xscape4u to allow us to perform the following (without detracting from the generality hereof):

- to pursue their business objectives and strategies;
- to comply with a variety of lawful obligations, including without detracting from the generality thereof, to carry out actions for the conclusion and performance of a contract as between Xscape4u company and the Data Subject;
- to put in place protective mechanisms to protect the parties' legitimate interests including the performance of risk assessments and risk profiles where applicable and necessary;
- to obtain or provide Personal Information from a credit bureau or credit provider or credit association, information about certain Data Subject's credit record, including personal information about any judgement or default history;
- for the purposes of contacting the Data Subject and attending to the Data Subject's enquiries and requests;
- for the purpose of providing the Data Subject from time to time with information pertaining to the Companies, their officers, employees, services and goods and other ad hoc business-related information;
- to pursue the parties' legitimate interests, or that of a third party to whom the Personal Information is supplied;
- for the purposes of providing, maintaining, and improving our Products and Services, and to monitor and analyze various usage and activity trends pertaining thereto;
- for the purposes of performing internal operations, including management of employees, employee wellness programmes, the performance of all required HR and IR functions, call centres, customer care lines and enquiries, attending to all financial matters including budgeting, planning, invoicing, facilitating, and making payments, making deliveries, sending receipts, and generally providing commercial support, where needed, requested, or required; and
- for the purpose of preventing fraud and abuse of the Companies' processes, systems, procedures, and operations, including conducting internal and external investigations and disciplinary enquiries and hearings.

For further information on data protection see below,

Description of categories of Data Subjects and personal information processed.

Xscape4u holds information and Records relating to the following broad categories of data subjects or persons, which is a non-exhaustive list of categories:

- Clients - Natural persons: names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; confidential correspondence.
- Clients – Juristic persons / entities / business partners: names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners.
- Clients – Foreign persons / entities: names; contact details; physical and postal, financial information addresses; date of birth; passport number tax related information; nationality; gender; confidential correspondence; registration number; founding documents; tax related information; authorised signatories, beneficiaries, ultimate beneficial owners.
- Contracted Service Providers/Suppliers/franchisors/franchisees - Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories, beneficiaries, banking information.
- Intermediaries/Advisor/Banks/Insurers /Agents; Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories, beneficiaries, ultimate beneficial owners.
- Employees / Directors /Potential Employees/Learners/Interns/Shareholders /Volunteers /Employees' family members/Temporary employees - gender, pregnancy; marital status; race, age, language, education information; financial information; employment history; ID number; next of kin; children's name, gender, age, school, grades; physical and postal address; contact details; opinions, criminal behaviour and/or criminal Records; well-being; trade union membership; external commercial interests; medical information; health Records; images; demographics.
- Website end-users/Application end-users: names, electronic identification data: IP address; log-in data, cookies, electronic localization data; cell phone details, GPS data, social media.
- Persons who interact with us physically or enter sites, offices, parking areas, manufacturing site, showroom and all facilities of the company or interact via websites / email / correspondence and who provide their personal information.

Categories of recipients for Processing personal information

We may supply personal Information to these potential recipients:

- Management.
- Employees and temporary employees/learnerships/internships/job applicants/agents/bursary applicants/directors.
- Business partners.
- Advertisers.
- Customers and clients.
- Medical Service Providers, insurance companies, pensions and provident funds, wellness, or health providers; banks.
- Contractors / vendors / suppliers / service providers / operators / franchisors / franchisees.
- Third party service providers.
- Cyber third parties service providers / Users / Third parties with whom Xscape4u conducts business.
- Statutory oversight bodies, regulators or judicial commissions of enquiry making a request for personal information, enforcement agencies; public bodies who we engage with to discharge legal and public duties and obligations including SARS, National treasury, Department of Labour and the financial sector conduct authorities.
- Courts, administrative or judicial forum, arbitration, statutory commission, or ombudsman making a request for personal information or discovery in terms of the applicable rules.
- Anyone making a successful Request for Access in terms of PAIA or POPIA.
- Subject to the provisions of POPIA and other relevant legislation, Xscape4u may share information about a client's creditworthiness with any credit bureau or credit providers industry association or other association for an industry in which Xscape4u operates.

We may from time to time have to disclose personal information to other parties as set out above, including, trading partners, agents, auditors, organs of state, regulatory bodies and / or national governmental, provincial, or local government municipal officials, or overseas trading parties or agents, but such disclosure will always be subject to an agreement which will be concluded as between ourselves and the party to whom we are disclosing the personal information to, which contractually obliges the recipient of the personal information to comply with strict confidentiality and data security conditions. Personal information may also be disclosed where we have a legal duty or a legal right to do so.

Cross border flows of personal information

Xscape4u may from time to time have to disclose a Data Subject's personal information to other parties, Such disclosure will always be subject to an agreement which will be concluded as between the company and the party to whom it is disclosing the Data Subject's personal information to, which contractually obliges the recipient of this personal information to comply with strict confidentiality and data security conditions. Where personal information and related data is transferred to a country which is situated outside the borders of South Africa, the Data Subject's personal information will only be transferred to those countries which have similar data privacy laws in place or where the recipient of the personal information is bound contractually to a no lesser set of obligations than those imposed by POPIA.

Security measures

Xscape4u will ensure that the Data Subject's personal information is securely stored electronically, which for operational reasons, will be accessible to certain categories of authorised persons within the company on a need to know and business basis, save that where appropriate, some of the Data Subject's personal information may be retained in hard copy and stored securely.

Considering the nature, scope, context, and purpose of Processing, Xscape4u ensure implementation of appropriate technical and organizational measures designed to ensure the confidentiality, integrity and security of personal information against unlawful access and against accidental loss, destruction or damage as prescribed by POPIA.

The security measures implemented to secure against unauthorized processing or access may include (note: this is not an exhaustive list):

- Firewalls; authentication software; intrusion detection systems; unique user profiles; encryption;
- Anti - Virus software and update protocols;
- Logistical and physical access control
- Secure setup of hardware and software making up our information technology infrastructure; and
- Outsourced service providers who are contracted to implement security controls.

9. REQUEST PROCEDURE

Completion of the prescribed form

Any Request for Access to a Record of a private body in terms of PAIA must substantially correspond with the form attached hereto marked *APPENDIX A - Request for Access to Record (Section 53(1) of PAIA) [this is per Regulation 7].*
Note: Section G to APPENDIX A requires you to explain how the record you are asking for is reasonably required for you to protect, or exercise, another right.

POPIA provides that a Data Subject may, upon proof of identity, request us to confirm, free of charge, all the information we hold about the Data Subject and may request access to such information, including information about the identity of third parties who have or have had access to such information.
POPIA also provides that where the Data Subject is required to pay a fee for services provided to him/her, we must provide the Data Subject with a written estimate of the payable amount before providing the service and may require that the Data Subject pays a deposit for all or part of the fee.

10. OBJECTION

POPIA provides that a Data Subject may object, at any time, to the Processing of personal information, on reasonable grounds relating to his/her situation, unless legislation provides for such Processing.
The Data Subject must complete the prescribed form attached hereto as *APPENDIX C - Objection to the Processing of personal information in terms of section 11(3) of POPIA Regulations relating to the protection of personal information, 2018 [this is per Regulation 2]* and submit it to the Information Officer at the postal or physical address or electronic mail address set out above.

11. RECTIFICATION

A Data Subject may also request us to correct or delete personal information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or destroy or delete a Record of personal information about the Data Subject that we are no longer authorised to retain Records in terms of POPIA's retention and restriction of Records provisions.

A Data Subject that wishes to request a rectification in the form of a correction or deletion of personal information or the destruction or deletion of a Record of personal information, must submit a request to the Information Officer at the postal or physical address or electronic mail address set out above, on the form attached hereto as *APPENDIX D – Request for correction or deletion of personal information or destroying or deletion of Record of personal information in terms of section 24(1) of POPIA's Regulations relating to the protection of personal information, 2018 [this is per Regulation 3].*

12. PROOF OF IDENTITY

Proof of identity is required to authenticate your identity and the Request for Access. You will, in addition to the prescribed form, be required to submit acceptable proof of identity such as a certified copy of your identity document or other legal forms of identity.

13. TIMELINES FOR CONSIDERATION OF A REQUEST FOR ACCESS

Requests will be processed within 30 (thirty) days, unless the request contains considerations that are of such a nature that an extension of the time limit is needed.
Should an extension be required, the initial 30 (thirty) days may be extended for a further period of no more than 30 (thirty) days, if for instance the request requires a search for records that cannot reasonably be completed within the initial period. You will be notified, together with reasons explaining why the extension is necessary.

14. GROUNDS FOR REFUSAL OF ACCESS AND PROTECTION OF INFORMATION

There are various grounds upon which a Request for Access to a Record may be refused. These grounds include:

- the protection of personal information of a third person (who is a natural person) from unreasonable disclosure;
- the protection of commercial information of a third party (for example: trade secrets; financial, commercial, scientific, or technical information that may harm the commercial or financial interests of a third party);
- if disclosure would result in the breach of a duty of confidence owed to a third party;
- if disclosure would jeopardise the safety of an individual or prejudice or impair certain property rights of a third person;
- if the Record was produced during legal proceedings, unless that legal privilege has been waived;
- if the Record contains trade secrets, financial or sensitive information or any information that would put us at a disadvantage in negotiations or prejudice it in commercial competition; and/or
- if the Record contains information about research being carried out or about to be carried out on behalf of a third party or by the Company.

Section 70 of PAIA contains an overriding provision. Disclosure of a Record is compulsory if it would reveal (i) a substantial contravention of, or failure to comply with the law; or (ii) there is an imminent and serious public safety or environmental risk; and (iii) the public interest in the disclosure of the Record in question clearly outweighs the harm contemplated by its disclosure. If the Request for Access to information affects a third party, then such third party must first be informed within 21 (twenty-one) days of receipt of the request. The third party would then have a further 21 (twenty-one) days to make representations and/or submissions regarding the granting of access to the Record.

15. REMEDIES AVAILABLE TO A REQUESTER ON REFUSAL OF ACCESS

If the Information Officer decides to grant a Requester access to the relevant Record, such access must be granted within 30 (thirty) days of being informed of the decision. There is no right of appeal against the decision of the Information Officer and the only recourse available to a Requester who is aggrieved by the decision of the Information Officer is by way of an application to a court for relief in terms of section 78 of PAIA.

16. APPENDICES – (FORMS)

APPENDIX A	Request for Access to Record
APPENDIX B	Outcome of Request and Fees Payable
APPENDIX C	Objection Form (POPIA)
APPENDIX D	Rectification (POPIA)

XSCAPE4U DATA PROTECTION POLICY

Xscape4u conduct business with the highest ethical standards and in compliance with all applicable privacy laws.

This Policy seeks to ensure that Xscape4u, The Company,:

- Complies with legal standards and best practices for the receipt, importing, processing, handling, storing, sharing and disposal of personal information belonging to individuals and legal entities ("data subjects"), which data subjects include without detracting from the generality thereof, employees, service providers, clients, and third parties;
- Protects the privacy rights of all data subjects with whom it engages/
- Is transparent in relation to the processing of personal data, especially in relation to what personal information it collects, the reasons for such collection and how it collects, handles, shares, stores and destroys such personal data; and
- Is aware of the risks in relation to the personal information including data breaches, unlawful access to personal data protection controls to manage data risks.

This policy follows suitable data protection procedures and standards when processing of personal data.

In line with the above this Policy sets out the following,

- The responsibilities under the data protection laws which apply in the areas where Xscape4u operates, and how it will comply with these policy laws;
- How Xscape4u processes personal data which is owned, applies to and/or relates to identifiable or identified individuals and legal entities, including employees, service providers, and other third parties, known as data subjects;

1 APPLICATION AND SCOPE OF THIS POLICY

1.1. This Policy applies to the following persons:

- all employees, who for the purposes of this Policy will include permanent, fixed term and temporary employees, directors, interns, third party representatives, agents and representatives who are carrying out work for or on behalf of the Xscape4u (hereinafter referred to as “employees”); and

1.2. The rules and standards set out in this Policy applies to all personal data processed by Xscape4u in an automated or non-automated manner, and regardless of how stored or recorded i.e. stored electronically, digitally, on paper or on other materials or through other methods.

1.3. All employees who process personal information on behalf of the Xscape4u are expected to comply with the company’s legal obligations in so far as they relate to the handling and processing of personal information, which has to be done in order to protect the company from the risk of non-compliance, and the consequences of such non- compliance, including loss of data, investigators, administrative penalties, criminal charges and fines, civil claims and damages, as well as reputational risk.

1.4. All employees who process personal information on behalf of Xscape4u must read, understand, and comply with its Policy when processing personal information in performing their tasks and must observe and comply with all personal information controls, practices, protocols and training to ensure such compliance.

1.5. Compliance with this Policy and related company policies and procedures is mandatory.

1.6. Any breach of this Policy and related policies and procedures may result in disciplinary action and the necessary corrective action.

2 DATA PROTECTION PRINCIPLES

The data processing laws are based on a set of core principles that Xscape4u comply to from the start of the information being collected until archived, deleted or destroyed.

2.1 Accountability

2.1.1 Xscape4u is responsible for and must be able to demonstrate compliance with the data protection principles and other obligations under the applicable data processing laws.

2.1.2 Xscape4u must ensure that it has adequate resources, systems, and processes in place to demonstrate compliance.

- Implementing organisational measures that are designed to ensure compliance with the data protection principles.
- ensuring that only personal information that is necessary for each specific purpose is processed both in relation to the nature, extent and volume of such personal data, the period of storage and the accessibility of the personal information.
- ensuring that where any intended processing presents a substantial risk to the rights and freedoms of data subjects, the Company has conducted an assessment of those risks and is taking steps to mitigate those risks.
- integrating data protection into Xscape4u internal procedures and documents, by way of privacy policies and processing notices.

2.2 Lawfulness, fairness, and transparency

Xscape4u must only process personal information in a lawful, fair and in a transparent manner.

2.3 Purpose limitation

Xscape4u must only collect and process personal information for a specified, explicit, and legitimate purpose.

2.4 Data minimisation

Xscape4u must ensure that personal information which is processed by it is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

2.5 Storage limitation

Xscape4u must ensure that personal information which is processed by it is not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

2.6 Security, integrity, and confidentiality

Xscape4eu must ensure that personal information which is processed by it is done in a manner that ensures its security using appropriate technical and organisational measures to protect the data against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

2.7 Transfers of personal information outside the Processing territories

Xscape4u must ensure that personal information which is processed by it is not transferred outside the borders of South Africa

2.8 Data subject rights and requests

Xscape4u must allow data subjects to exercise their rights in relation to their personal data.

3 PROCESSES IMPLEMENTED BY THE COMPANY IN ORDER TO ENSURE THAT THE DATA PROTECTION PRINCIPLES ARE GIVEN EFFECT TO

3.1 Lawfulness and consent to process under certain circumstances

3.1.1 Consent to process a data subject's personal information will not always be required. Xscape4u in terms of the data processing laws will be allowed to lawfully process a data subject's personal information without the data subject's consent under the following circumstances:

- The processing is necessary for conclusion of the performance of a contract to which the data subject is a party (for instance a contract of employment or registration with the Company as a vendor);
- The processing is necessary in order for the Company to comply with certain legal obligations (for instance, to comply with the labour laws);
- The processing is to protect the legitimate or vital interests of the data subject.
- The processing is to perform a public duty or to perform tasks conducted in the public interest or the exercise of official authority.

3.1.2 Where the processing of a data subject's personal information is required, we need to ensure that such processing is lawful and that the data subject must agree to such processing, i.e. it has to provide consent.

3.1.3 Furthermore, where consent is required from the data subject, then such consent must be freely and genuinely given.

3.1.4 Where, in terms of the data processing laws, consent to process a data subjects' personal information is required, such consent may at any time be withdrawn by the data subject. If consent is withdrawn, then the Company will no longer be allowed to continue processing such personal information from the date of such withdrawal and so it will be important to advise the data subject of the consequences of the withdrawal, i.e. that the Company will not be able to continue its relationship with the data subject.

3.1.5 Where a third party provides the Company with another's personal information (for example, CV's housing a job applicant's personal information provided by a recruitment agent or credit bureau records housing personal data about a creditor which is provided by a credit bureau in relation to a data subject's credit worthiness or where personal information pertaining to a service provider's employee is provided by a service provider) the Company must obtain confirmation that it was collected by the third party in accordance with the data privacy law requirements and that such personal information was lawfully processed, and that the sharing of the personal information with the Company was clearly explained to the data subject by such third party and where required, permission to process including the passing on or the sharing of information was obtained from the owner thereof.

3.1.6 The data processing laws distinguish between personal information and "special personal information" which is also known as "sensitive personal data". Special personal data concerns the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.

3.1.7 Under the GDPR to process special personal information at least one of the following conditions must be met:

- the data subject must consent to the processing of such data for one or more specified purposes;
- the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the Company or of the data subject in the field of employment, social security, and social protection law;
- the processing is necessary to protect the legitimate interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- the Company is an entity with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that entity or to persons who have regular contact with it in connection with its purposes and that the personal information is not disclosed outside the entity without the consent of the data subjects;

- the processing relates to personal information which is clearly made public by the data subject;
- the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;

3.1.8 Under POPIA, in order to process special personal information, being the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings, the following has to be shown in relation to such processing:

- the processing is carried out with the consent of a data subject;
- the processing is necessary for the establishment, exercise or defense of a right or obligation in law;
- the processing is necessary to comply with an obligation of international public law;
- the processing is for historical, statistical or research purposes, to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned; or it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
- the information has deliberately been made public by the data subject;
- permission has been received from the Information Regulator to process special personal information if such processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the data subject;
- where the processing concerns religious or philosophical beliefs, and such processing has been done and is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing, and provided that such information is not supplied to third parties without the consent of the data subject;

- where the processing concerns race or ethnic origin, and such processing is carried out to identify data subjects and only when this is essential for that purpose; and to comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination;
- collective agreements which create rights dependent on the health or sex life of the data subject; or (ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity, and provided that such information is kept confidential;

3.1.9 Directors, employees, and others processing personal information on behalf of the Company must only process special personal information if it is able to justify such processing as described above. Processing special personal information without the data subjects' consent, or where such processing cannot be justified, may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.

3.2 Purpose specific

3.2.1 The Company, including directors, employees and others processing personal information on behalf of the Company must only collect and process personal information for specified, explicit and legitimate purposes that have been communicated to data subjects before the personal information is collected.

3.2.2 When collecting and using a data subject's personal data, the Company, including its directors, employees and others processing personal information on behalf of the Company, have a duty to inform the data subject why the information is required and what will be done with it whilst under the Company's control. No data subject should be surprised to learn that their personal information has been collected, consulted, used, or otherwise processed by the Company. Any use or processing of a data subject's personal information must be purpose specific, and the data subject must be told about such processing and how such data will be used before the intended use of the data. The processing of a data subject's personal information will only be lawful if the data subject has been provided with an explanation for the processing, including the purpose, which must be:

- specific (not given in respect of multiple unrelated purposes);
- informed (explained in plain and accessible language);
- unambiguous and given by a clear affirmative action (meaning opt-in; silence, inactivity or pre-ticked boxes will not be sufficient); and
- separate and unbundled from any other terms and conditions provided to the data subject.

3.2.3 The Company, its directors, employees, and other processing personal information on behalf of the Company must ensure that they do not process any personal information obtained for one or more specific purposes for a new purpose that is not compatible with the original purpose. If the Company, or its directors, employees and others processing personal information on behalf of the Company want to process additional personal information for a new purpose for which the personal information was collected, then they will have to provide the data subject with the details of such processing and the reason(s) why the data has to be processed, and where necessary, if required, obtain the data subject's consent to such processing.

3.3 Data minimisation

3.3.1 The personal information that the Company or its directors, employees and others processing personal information on behalf of the Company collect and process must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is to be processed.

3.3.2 Directors, employees, and others processing personal information on behalf of the Company must only process personal information that is absolutely necessary for the performance of the required purpose and related duties and tasks and not for any other purposes.

3.4 Accuracy

3.4.1 The personal information that the Company it's directors, employees and others processing personal information on behalf of the Company collect and process must be accurate and, where necessary, kept up-to-date and must be corrected and deleted without delay when the Company or its directors, employees and others processing personal information on behalf of the Company discover, or are notified, that the data is inaccurate.

3.4.2 Directors, employees, and others processing personal information on behalf of the Company must ensure that they have procedures in place to ensure that the personal information on record remains updated, especially where one becomes aware that personal information is inaccurate. Where appropriate, any inaccurate or out-of-date records should be deleted, or destroyed.

3.5 Security, integrity, and confidentiality

3.5.1 The personal information that the Company, its directors, employees, and others processing personal information on behalf of the Company collect and process must be secured by appropriate technical and organisational measures which guard against accidental loss, destruction, or damage, and against unauthorised or unlawful processing.

- Directors, employees, and others processing personal information on behalf of the Company must ensure that they observe and comply with all the Company's information security policies, especially those pertaining to personal information security at all times.
- do not attempt to circumvent any administrative, physical, or technical measures the Company has implemented as doing so may result in disciplinary action and in certain circumstances, may constitute a criminal offence, give rise to civil liability or administrative penalties.
- ensure that the confidentiality and security of personal information is always maintained.
- ensure that they only store personal information on Company servers which are protected by approved security software.
- ensure that prescribed security measures and controls are implemented, or where instructed, followed to prevent all and any unauthorised access to personal information, the accidental deletion of personal information or the exposure of personal information to malicious hacking attempts.
- ensure that all devices where personal information is stored, are password protected and that passwords are not written down or shared, irrespective of seniority or department which passwords must be strong passwords which are changed regularly. If a password is forgotten, it must be reset using the applicable method.
- ensure that all hard copies of personal data, along with any electronic copies stored on physical or removable media is stored securely in a locked box, drawer, cabinet, or similar, and that such data is not removed from the Company premises unless with prior approval from the data subject's departmental head and when so removed, that such data is encrypted if it is on a removable media device.

- ensure that where personal information is stored on paper, that it is not left in places where persons can view the data, e.g. on a printer, but instead is kept in a secure place where an unauthorised person cannot access or see it, such as in a locked drawer, safe or cabinet and that when no longer required, that same is shredded;
- ensure that personal information is not transferred or sent to any entity not authorised directly to receive it.

- ensure that where personal information is transferred physically, whether in hardcopy form or on removable electronic media, that it is passed directly to the recipient or sent using recorded delivery services and housed in a suitable container marked “confidential”;
- ensure that generally all personal information is handled with care at all times, kept confidential, and that it is not left unattended or on view to unauthorised employees; and
- ensure that all software (including, but not limited to, applications and operating systems) used in connection with the Company are installed on Company owned computers or devices and which have been installed by and with the prior approval of the IT department, which software must at all times be kept up to date.

3.6 Retention of personal information

3.6.1 Storing personal information for longer than necessary may increase the severity of a data breach and may also lead to increased costs associated with such storage in order to manage these risks the Company will maintain policies and procedures to ensure that personal information is deleted, destroyed or anonymised after a reasonable period of time following expiry of the purpose for which it was collected.

3.6.2 Where appropriate, directors, employees and others processing personal information on behalf of the Company must take all reasonable steps to delete or destroy any personal information that the Company no longer requires in accordance with the relevant Company’s records management policies and data retention and destruction policy.

3.7 Sharing personal data

3.7.1 The transfer of any personal information to an unauthorised third party will give rise to and constitute a breach of the lawfulness, fairness, and transparency principle and, where caused by a security breach, will give rise to and constitute a personal information breach.

3.7.2 Directors, employees, and others processing personal information on behalf of the Company are not permitted to share personal information with third parties, unless:

- there is a legitimate company need to share the personal data.
- the fact that the personal information will be shared with another has been communicated to the data subject in a privacy notice or processing notice beforehand; and
- the person receiving the personal information has either agreed to keep the personal information confidential and to use it only for the purpose for which it was shared under a data transfer agreement, or where acting as an operator or a processor, (i.e. such person will be processing the personal information on behalf of the Company), has concluded an Operator Agreement with the Company, before receipt of the personal data.

3.8 Transparency and processing notices

3.8.1 The Company has a duty to show that it has dealt with a data subject in a transparent manner. To demonstrate transparency, the Company must provide all data subjects with appropriate privacy notices or processing notices before it collects and processes their personal data.

3.8.2 Whenever a director, employee and or any other representative processes personal information on behalf of the Company, such person must ensure that the data subject is made aware of the information set out below:

- the types of personal information collected and the purpose or reason for the collection.
- the lawful basis relied upon for such processing or whether consent is required for the processing.
- the period for which the personal information will be retained.

3.9 Data subject rights and requests

- The data processing laws provide data subjects with a number of rights in relation to their personal data, including the right to access its data, and to change it.
- The Company has developed, implemented, and will maintain certain processes which give effect to these data subject rights, as described below, which processes will be directed to and handled directly by the relevant Company's Data Processing Officer, Information Officer or his or her deputy, and no other.
- All directors, employees and persons processing personal information on behalf of the Company must take note of and give effect to these processes as described below.

3.9.1 The right to withdraw consent.

- Where a data subject has had to give its consent to the processing of its personal data, the data subject in such case will have the right to withdraw such consent at any time, which withdrawal will apply from the date of withdrawal only and which will not affect the legality of the processing of its personal information to which the consent applies prior to the withdrawal.
- To give notice of the withdrawal of consent, the data subject must complete the standard Company "withdrawal of consent notice" form

3.9.2 The right to be informed.

- A data subject has the right to be told why its personal information is being processed, including what type of personal information will be processed, the reason for the processing, who the personal information will be shared with and whether such information will be sent outside the territory where it is being processed or held, and how the personal information will be safeguarded.
- In order to give effect to this right, the Company has developed a series of processing or privacy notices which are described under section 3.9 above.
- Directors, employees and/or any other representatives who processes personal information on behalf of the Company, in order to give effect to a data subject's right to be informed, must ensure that all documents and/or records where personal information is recorded and/or housed or which calls for or sets out that personal information or information is required, house a data processing clause which records or states in such document or record, that personal information will be processed and that such processing is subject to the Company's standard processing or privacy notices.

3.9.3 The data subject's right to have access to its personal data.

- All data subjects have the right at any time to ask any person or entity who holds its personal data, including the Company, for access to their personal data, including finding out more about the personal information which the Company holds about them, what it is doing with that personal data, and why it is processing the personal data.
- In South Africa, in terms of POPIA, this has to be exercised using the "request for access to information" procedure which is described under a law known as the Promotion of Access to Information Act, 2000 (PAIA) and which request procedure is more fully set out under the PAIA Manual.
- All request for information held by the Company, including personal information has to be made using the standard request procedure referred to above, which request will be submitted directly to, and which will be handled directly by, the Company, in accordance with the provisions of PAIA.

3.9.4 Rectification of personal data

- All data subjects have the right to request that their personal information is updated or rectified where it is inaccurate, incomplete, or out of date. The standard Company “rectification” form (Form 2) for requests is available.
- The relevant company Data Protection Officer or the Information Officer on receipt of the request, provided it is submitted on the prescribed form, will where able, rectify as far as possible, the personal information in question, and inform the data subject of the rectification. Furthermore, if any affected personal information has been disclosed to third parties, those parties will also be informed of any such rectification and the reasons therefor.

3.9.5 The right to object and/or restrict processing.

- Data subjects have the right to object to the Company processing their personal information based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company has legitimate grounds for such processing which override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the performance of a legal or statutory duty or the conduct of legal claims.
- Where a data subjects objects to the Company processing its personal information for direct marketing purposes, the Company must immediately stop any further direct marketing.
- A data subject furthermore has the right to object to the processing of its personal information coupled with the right to ask the Company to restrict processing the personal information where the data subject:
    - believes that the personal information is inaccurate.
    - believes that the processing was unlawful, and the data subject prefers restriction of processing over erasure.

- believes that the personal information is no longer necessary in relation to the purposes for which it was collected but one is required to establish, exercise, or defend a legal claim and needs to retain the data; or
- has objected to the processing pending a determination whether the Company's legitimate interest's grounds for processing the personal information override those of the data subject.

- In accordance with the above, the data subject may object to, and ask the Company to place a restriction on the processing of the personal information which the Company holds, which request must be made using the standard Company "objection" form (Form 1), available.
- If the relevant Data Protection Officer or Information Officer, as applicable in the circumstances is in agreement with and succumbs to the request of the data subject, then the Company shall pend any further processing of the personal information in question and retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further.
- If any affected personal information has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

3.9.6 The right to data portability

- This is the right of the data subject to receive or ask the Company to transfer to a third party, a copy of the data subject's personal information in a structured, commonly used machine-readable format.
- To facilitate the right of data portability, the data subject must complete the standard Company "data portability" form (Form 4). All requests for copies of personal information shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

3.9.7 The right to object to direct marketing

- A data subject who has opted into any form of direct marketing has the right to opt out from any subsequent direct marketing, i.e., it has the right to ask the Company not to process its personal information for any further direct marketing purposes.
- A data subject can either submit its request using the prescribed objection notice (see notice referred to under the second point of section 3.10.5 above or alternatively simply use the opt out request which the Company is obliged to include in all its electronic direct marketing communications.

3.9.8 The right to object to decisions based solely on automated processing including Profiling.

- A data subject has the right to object to decisions creating legal effects or significantly affecting the data subject which were made solely by automated means, including profiling, and the right to request human intervention.
- The data subject also has the right to ask for the reasons why a decision was made and the underlying methodology which was used to make the decision which request must be made by completing and submitting the standard Company "objection" form which is available.

3.9.9 The right to erasure (right to be forgotten)

- A data subject has the right to request that the Company erases the personal information which the Company holds about it in the following circumstances:
    - it is no longer necessary for the Company to hold that personal information with respect to the purpose(s) for which it was originally collected or processed.
    - the data subject wishes to withdraw its consent.
    -
    - the data subject objects to the Company holding and processing its personal information (and there is no overriding legitimate interest to allow the Company to continue doing so);
    - the personal information has been processed unlawfully; or
    - personal information needs to be erased for the Company to comply with a particular legal obligation.

- Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject must be informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the employee data subject shall be informed.

- If any personal information that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

3.9.10 The right to be notified of a personal information breach.

- A data subject must be notified of a personal information breach which involves its personal data, which notice will be prepared by and conveyed to affected data subjects by the relevant person.

3.9.11 The right to complain.

- A data subject has the right to lodge a complaint or objection with regards to the processing of its personal data, which complaint or objection must set out and concern a non-compliance by the Company with the data processing principles or concern a non-compliance with the data processing laws.
- The data subject is encouraged to make use of the standard Company "objection" form (Form 1) available.
- On receipt of the complaint or objection, the relevant Company Data Processing Officer or Information Officer will attempt to hear and resolve the matter and failing resolution will provide the data subject with a non- resolution notice.
- If the Data Processing Officer or the Information Officer and data subject can resolve the matter, a record setting out the solution will be complied, and signed by the parties and any other affected persons provided with details of the resolution.
- Where the parties are unable to resolve the matter, the data subject on receipt of the abovementioned notice will have the right to refer the complaint onwards, in the case of an alleged POPIA breach or infringement to the Information Regulator, or in the case of an alleged GDPR breach or infringement to the Information Commissions Officer or another appropriate supervisory authority.
- In order to give effect to the above, all directors, employees and/or any other representatives who processes personal information on behalf of the Company, must familiarise themselves with these rights and the related processes, and ensure that all data subjects are informed of these rights and the procedure which has to be followed when a data subject wishes to make use of these rights.

3.10 Direct marketing

3.10.1 The Company and its directors, employees and/or other representatives who processes personal information on behalf of the Company must ensure that before they send direct marketing to customers for the first time, that they have given the customer the opportunity in an informal manner to agree or disagree to the receipt of direct marketing material.

3.10.2 The Company and its directors, employees and/or other representatives who process personal information on behalf of the Company must ensure that before they send direct marketing to non-customers that they receive appropriate opt in consents in the prescribed manner and form as per the provisions of POPIA.

The Company and its directors, employees and/or any other representatives who process personal information on behalf of the Company must ensure that when a data subject exercises their right to object to direct marketing, in the form of an opt out, that such opt out is recorded and honoured.

3.11 Operators

3.11.1 An operator (as defined under POPIA) or a processor (as defined under the GDPR) is an entity who processes personal information on behalf of the Company without coming under its direct control.

Under POPIA where the Company makes use of an Operator, in terms of section 19 – 21 of POPIA, it must ensure that the Operator only uses the Personal Information as per the mandate to process issued by the particular Company; keeps the Personal Information placed under its control, confidential, secure and safe, and notifies the Responsible Party of unauthorised access by an unauthorised person. The aforesaid to be contained in a written agreement/or an Operator Agreement / Addendum (the latter to amend any existing contract) between the Company and the Operator, which agreement sets out the above provisions and any other terms and rules the Operator will have to follow when processing Personal Information on behalf of the Company.

Under GDPR all processors must conclude a written contract that binds the processor to the controller in respect of the processing activities. The Controller (Responsible Party) shall only use Processors (Operators) at provide adequate guarantees to implement appropriate technical and organisational measures to protect the personal information. The processor is to conclude the particular Company's standard data transfer contract (or Operator Agreement) prior to them receiving and or processing personal information on behalf of the particular Company, which agreement houses the rules which will have to be followed by the processor in order to ensure that such data is processed and protected in accordance with the data processing laws and Company's security procedures and standards.

3.11.2 Directors, employees or persons who process personal information on behalf of the Company must ensure that when they appoint an operator (as defined under POPIA) or a processor (as defined under the GDPR) that the relevant standard data transfer contract or Operator Agreement is concluded with such operator or processor prior to them receiving and or processing personal information on behalf of the Company.

3.12 Profiling

3.12.1 The Companies from time to time, use personal information for profiling purposes which is done via "cookies" on their company websites.

3.12.2 Directors, employees, or persons who process personal information on behalf of the Company, must ensure that when personal information is used for profiling purposes, that the following takes place:

- clear information explaining the profiling is provided to data subjects, via privacy notices, cookie opt ins and cookie notices, including the significance and consequences of the profiling.
- Appropriate mathematical or statistical procedures are used.
- Technical and organisational measures are implemented to minimise the risk of errors. If errors occur, such measures must allow the errors to be easily corrected; and
- All personal information processed for profiling purposes shall be secured to prevent discriminatory effects arising out of profiling.

3.13 Record-keeping

3.13.1 The Company must keep full and accurate records of all its processing activities in accordance with the data processing laws and related requirements including:

- all processors and/or operators (operator register) who process personal information on behalf of the Company.
- the purposes for which the Company collects, holds and processes personal data;
- details of the categories of personal information collected, held and processed by the Company;
- details of any transfers of personal information to non-South African, UK or non-EEA operations situated in countries outside the EEU, the UK and South Africa, including all mechanisms and security safeguards.
- details of all retention periods in respect of personal information as per the Companies data retention and destruction policy; and
- detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

3.14 Archiving and destruction of data

3.14.1 The Company to facilitate the correct creation, use, storage, archive, retrieval, and ultimate destruction of records has developed a records management and retention policy and records retention schedule.

3.14.2 Directors, employees, and others processing personal information on behalf of the Company must ensure that when they process personal data, that such data is processed in strict compliance with the Company's records management and retention policy and records retention schedule.

3.14.3 Directors, employees and others processing personal information on behalf of the Company must furthermore ensure that when personal information is no longer needed for the specific purposes for which it was collected, that such personal information is archived for the legally required retention period and thereafter deleted, destroyed or anonymised, which must be done in strict compliance with the particular Company's retention Policy and records retention schedule.

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

APPENDIX B

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	R2.00		
Printed copy	R2.00		
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 quotation from 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 _____

_____

Signature Information officer

APPENDIX C

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 …… on this ……. day of …… 20 ……..

……

Signature of data subject / designated person

RECTIFICATION

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 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.*

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 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**

D	**REASONS FOR *CORRECTIONS 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 …… on this ……. day of …… 20……..

…….
Signature of data subject / designated person