MANUAL IN TERMS OF SECTION 51
OF THE
PROMOTION OF ACCESS TO INFORMATION ACT, 2 OF 2000
("PAIA"/"THE ACT")

INDEX

1. INTRODUCTION

1.1 MLA Theatrical Agents cc t/a MLA ("Company"), is a legal entity and/or incorporated in the Republic of South Africa and operates as *inter alia* artists agency.

1.2 This Manual has been compiled in accordance with the requirements of the Promotion of Access to Information Act, Act No. 2 of 2000 ("the Act"). The Manual contains the information specified in section 51(1) of the Act, which is applicable to the Company as a private body. This information is as follows:

1.2.1 the contact details of the head of the private body;

1.2.2 a description of the guide referred to in section 10 of the Act;

1.2.3 the latest notice published by the Minister under section 52(2) of the Act;

1.2.4 a description of the records of each private body which are available in terms of the terms of any legislation other than the Act;

1.2.5 a description of the subjects on which each private body holds records and the categories of records held on each subject in sufficient detail to facilitate a request for access to a record; and

1.2.6 other information as prescribed by regulation.

1.3 The Manual will be updated on a regular basis in accordance with the requirements of section 51(2) of the Act.

1.4 In this Manual, the following words bear the meaning set out below:

- "BEE" means black economic empowerment;
- "Client" means a natural or juristic person who or which receives services from the Companies;
- "Company means MLA SA with registration number 1988/022386/23, a company incorporated in accordance with the Laws of the Republic of South Africa;
- "Employee" means any person who works for or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration;
- "Guide" means the guide published by the SAHRC in terms of section 10 of the Act;

- "the/this Manual" means this Manual which is published in accordance with section 51 of the Act and "this Manual" shall have the same meaning;
- "the Minister means the Cabinet member responsible for the administration of justice, presently the Minister of Justice and Constitutional Development;
- "Personal Information" means the information of a data subject as defined in the Protection of Personal Information Act, 2013, section 1: 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable existing juristic person, including, but not limited to—
  - information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;
  - information relating to the education or the medical, financial, criminal or employment history of the person;
  - any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier, or other assignment to the person;
  - the biometric information of the person;
  - the personal opinions, views, or preferences of the person;
  - correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
  - the views or opinions of another individual about the person; and
  - the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

- "POPIA" means the Protection of Personal Information Act, 2013
- "Requester" means any person or entity requesting access to a record that is under the control of the Company;
- "SAHRC" means the South African Human Rights Commission;
- "the Act" means the Promotion of Access to Information Act, Act No. 2 of 2000 (as amended);
- "Head of the Company" means the General Managers of the Company, or any person duly authorised by him or her to carry out the duties ascribed to the "head" of a private body by the Act.

2. CONTACT DETAILS

The General Managers of the Companies are as stated below and are the heads of the respective Companies for the purposes of the Act and are the persons to whom requests for access to records should be addressed.

- **Name of General Manager**: Nina Morris (CEO)
- **Physical address of the Company**: MLA House, 14 Clamart Road, Richmond, 2092, JHB,
- **Postal address of the Company**: PO Box 41792, Craighall, Johannesburg, 2024
- **Telephone of the Company:** +27 87 806 6970
- **E-mail address of the head of the Company**: Nina@mlasa.com / Privacy@mlasa.com

3. SECTION 10 GUIDE ON HOW TO USE THE ACT

3.1 The SAHRC has, in terms of section 10 of the Act, published a Guide to assist persons wishing to exercise any rights in terms of the Act.

3.2 The Guide may be obtained from the SAHRC. Any person wishing to obtain the Guide may either access it through the website of the SAHRC at www.sahrc.org.za or should contact:

- PAIA Unit
- Research and Documentation Department
- South African Human Rights Commission
- Private Bag X2700, Houghton, 2041

- Telephone: (011) 877 3600
- Fax: (011) 403 0625
- Email: PAIA@sahrc.org.za

4. RECORDS AVAILABLE IN TERMS OF ANY OTHER LEGISLATION

4.1 Certain records held by the Companies are available in terms of legislation other than the Act.

4.2 The specific records which are available in terms of such legislation are set out therein and these records may in certain instances only be accessed by the persons specified in the relevant legislation. The legislation is as follows:

- Basic Conditions of Employment Act, Act No. 75 of 1997;
- Companies Act, Act No. 71 of 2008;
- Compensation for Occupational Injuries and Diseases Act, Act No. 130 of 1993;
- Competition Act, Act No. 89 of 1998;
- Consumer Protection Act, Act No. 68 of 2008;
- Employment Equity Act, Act No. 55 of 1998;
- Fertilizers, Farm Feeds, Seeds and Remedies Act, Act No. 36 of 1947;
- Foods, Cosmetics and Disinfectants Act, Act No. 54 of 1972;
- Income Tax Act, Act No. 58 of 1962;
- Labour Relations Act, Act No. 66 of 1995;
- Legal Metrology Act, Act No. 9 of 2014;
- Measurement Units and Measurement Standards Act, Act No. 18 of 2006;
- Medical Schemes Act, Act No. 131 of 1998;
- National Consumer Act, Act No. 34 of 2005;
- National Regulator for Compulsory Specifications Act, Act No. 5 of 2008;
- Occupational Health and Safety Act, Act No. 85 of 1993;
- Pension Funds Act, Act No. 24 of 1956;
- Protection of Personal Information Act, Act No. 4 of 2013;
- Skills Development Act, Act No. 97 of 1998;

- Skills Development Levies Act, Act No. 9 of 1999;
- Unemployment Insurance Act, Act No. 63 of 2001;
- Unemployment Insurance Contributions Act, Act No. 4 of 2002;
- Value Added Tax Act, Act No. 89 of 1991.

5. DESCRIPTION OF THE SUBJECTS ON WHICH THE COMPANY HOLDS RECORDS AND THE CATEGORIES OF RECORDS HELD ON EACH SUBJECT

5.1 The procedure in terms of which such records may be requested from the Company is set out in Section 7 of this Manual. The records listed below will not in all instances be provided to a requester who requests them in terms of the Act. The requester should show that he or she has the right in terms of the Act to be given access to the records in question.

5.2 Categories of records and description of records held-

5.2.1 Administration, Secretarial and Legal:

- Shareholder records;
- Share register;
- Minutes of meetings of directors;
- Records relating to the incorporation of the Companies;
- Minutes of meetings of committees and sub-committees;
- Power of Attorney;
- Record of major litigation/arbitration proceedings;
- Insurance policies;
- Title deeds;
- Mortgage bonds;
- Trademark, copyright, patent, service mark certificates and registrations.

5.2.2 Management:

- Minutes of meetings of Executive Committee;
- Internal correspondence;
- Resolutions of the directors of the Companies.

5.2.3 Finance:

- Accounting records;
- Tax records;
- Debtors' records;
- Creditors' records;
- Insurance records;
- Auditors' reports;
- Interim and annual financial statements;
- Bank statements and other banking records for business and trust accounts;
- Invoices issued in respect of debtors and billing information;
- Records regarding the Companies' financial commitments.

5.2.4 Human Resources:

- List of employees;
- Statistics regarding employees;
- Employment contracts;
- Conditions of employment;
- Information relating to prospective employees;
- Personnel records including personal details, disciplinary records, performance, and internal evaluation records;
- CCMA records;
- Registrations with Department of Labour: UIF, COIDA and Skills Development Levies Act;
- Employee tax information;
- Records of Unemployment Insurance Fund contributions;
- Records regarding group life assurance and disability income protection;
- Provident fund records;

- Payroll records;
- Health and safety records;
- Workplace skills plans;
- Codes of conduct;
- Disciplinary code and procedure;
- Grievance procedure;
- Appeal procedure;
- Remuneration policy;
- Training schedules and material;
- Internal policies and procedures regarding dismissals, performance appraisal, recruitment, selection, advertising of positions, appointments, retirement, promotions, leave, extended sick leave, study leave, salaries, overtime, bonuses, medical aid, health and safety, adoption leave and benefits, BEE procurement, loans, working parents, black economic empowerment, smoking, use of company resources including telephones, motor vehicles and computers, sexual harassment, HIV-Aids and Pro Bono policy;
- Correspondence relating to personnel.

5.2.5 Supplier

- Supplier lists and details of suppliers;
- Agreements with suppliers

5.2.6 Information Technology Department

- Computer software;
- Support and maintenance agreements;
- Records regarding computer systems and programmes;
- User Manuals and licenses

5.2.7 Property

- Asset registers;
- Lease agreements in respect of immovable property;
- Records regarding insurance in respect of movable property;
- Records regarding insurance in respect of immovable property

5.2.8 Procurement

- Records of tenders and vendor applications;
- Policy and procedure of tenders

5.2.9 Supply Services

- Supply services lists with freight providers and details of freight haulers;
- Agreements with Freight Haulers;
- Claim process records;
- Records of delivery and dispatch of company products

5.2.10 Marketing Department

- Marketing, advertising, and promotional material of products.

5.2.11 Research and Development

- Records of various laboratory tests, reports, research, and development material on household and pharmaceutical products.

5.2.12 Sales Department

- Records of agreements, invoices, rebate structures and pricing with customers and distributors;
- Credit applications;
- Customer and Distributor details

5.2.13 Safety, Health and Environment

- Complete Safety, Health and Environment Risk Assessment;
- Environmental Managements Plans;
- Inquiries, inspections, examinations by environmental authorities.

5.2.14 Corporate Affairs

- Records of all donations to education and society.

5.2.15 Miscellaneous

- Internal correspondence;
- Firm publications.

6. CATEGORIES OF RECORDS WHICH ARE AVAILABLE WITHOUT REQUEST

6.1 No notices relating to the Companies have been published by the Minister in terms of section 52(2) of the Act.

6.2 Certain records are available without needing to be requested in terms of the request procedures set out in the Act and detailed in Section 7 of this manual. This information may be inspected, collected, purchased, or copied (at the prescribed fee for reproduction) at the offices of the Companies. Certain information is also available on the Company's website – MLASA.com. The records include:

- Marketing brochures;
- Company and Product websites;
- Product content on Social Media;
- Product Information;
- Usage Instructions.

7. REQUEST PROCEDURE IN TERMS OF THE ACT

7.1 A request for access to records held by the Company/(ies) in terms of section 50 of the Act must be made on the form contained in the Regulations Regarding the

Promotion of Access to Information (Form C). A copy of the form is attached as Annexure A to this manual. The request must be made to the Company/(ies) at the address, or email address, specified in Section 2 above.

7.2 A requester must provide sufficient detail on the prescribed form to allow the Company/(ies) to identify the record or records which have been requested and the identity of the requester. If a request is made on behalf of another person or entity, the requester must submit details and proof of the capacity in which the requester is making the request, which must be reasonably satisfactory to the Company/(ies). The requester is also required to indicate the form of access to the relevant records that is required, and to provide his, her or its contact details in the Republic of South Africa.

7.3 The requester must identify the right that he, she, or it is seeking to exercise by accessing records held by the Company/(ies) and must explain why the record or records requested is or are required for the exercise or protection of that right.

7.4 The Company/(ies) may, and must in certain instances, refuse access to records on any of the grounds set out in Chapter 4 of Part 3 of the Act which include: that access would result in the unreasonable disclosure of personal information about a third party, that it is necessary to protect the commercial information of a third party or the Company/(ies) itself, that it is necessary to protect the confidential information of a third party, that it is necessary to protect the safety of individuals or property, that a record constitutes privileged information for the purpose of legal proceedings, and that it is necessary to protect the research information of a third party or the Company/(ies) itself. Access to documents may also be refused on the basis of professional privilege.

7.5 The Company/(ies) is required to inform a requester in writing of its decision in relation to a request. If the requester wishes to be informed of the Company's decision in another manner as well, this must be set out in the request and the relevant details included, to allow the Company to inform the requester in the preferred manner.

7.6 The Company/(ies) will make a decision in relation to a request for records within 30 days of receiving it, unless third parties are required to be notified of the request or the 30-day period is extended as provided for in the Act. The Company/(ies) will notify the requester if the 30-day period for processing a request is to be extended.

7.7 Where a request is refused, a requester may apply to the High Court within 30 days of being informed of the refusal of the request, for an order compelling the record or records requested to be made available to the requester or for another appropriate order. The Court will determine whether the records should be made available or not. Notwithstanding the above, a requester may lodge a complaint to the Information Regulator (the complaint must be made in writing), against the access fee to be paid or the form of access granted, as referred to in terms of section 63(3) and 74(2) – the format of the complaint is available on the Information Regulator's website and can also be requested from the Company directly. The

Information Regulator is required to give reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Information Regulator, to put the complaint in writing.

8. FEES PAYABLE

8.1 A requester has to pay a request fee of R50.00, other than where the requester is seeking access to a record containing personal information about him, her, their or itself. The requester may lodge a complaint to the Information Regulator as described above, against the access fee to be paid or the form of access granted. If the requester is seeking reproduction of a record containing personal information, then a fee may be charged. This request fee may be paid at the time a request is made, or the person authorised to deal with such requests on the Company's/(ies)' behalf may notify the requester that he, she, them or it needs to pay the request fee before processing the request any further. A requester may apply to Court to be exempted from the requirement to pay the request fee.

8.2 Where a request for access to a record or records held by the Company/(ies) is granted, the requester also has to pay an access fee for the reproduction of the record or records, and for the search for and the preparation of the records for disclosure. The Company/(ies) is entitled to withhold a record until the required access fees have been paid. The access fees which are payable are as follows:

Photocopy of an A4-size page or part thereof	R1.10
Printed copy of an A4-size page or part thereof held on a computer or in electronic or machine-readable form	R0.75
For a copy in a computer-readable form on USB	R7.50
Transcription of visual images, for an A4-size page or part thereof	R40.00
Copy of visual images	R60.00
Transcription of an audio record, for an A4-size page or part thereof	R20.00
Copy of an audio record	R30.00
In addition, if the search for and preparation of the record or records requested takes more than six hours, the Company/(ies) may charge R30.00 for each hour or part thereof which is required for the search for and preparation of the records.	

8.3 If the Company/(ies) is of the opinion that the search for and the preparation of the records requested will require more than six hours, the Company/(ies) is entitled to ask for a deposit of one third of the access fees which will be payable in respect of the records requested by the requester. The requester may make an application to Court to be exempted from the requirement to pay this deposit. If a deposit is made and access to the records requested is subsequently refused, the deposit will be repaid to the requester.

9. OTHER INFORMATION AS PRESCRIBED

The Minister has not prescribed that any further information must be contained in this manual.

10. PROCESSING OF PERSONAL INFORMATION

The purposes for which the Companies process or will process Personal Information is to allow the Companies to ensure that it best aligns the consumer's needs with the services available, OR otherwise as is provided for under lawful processing in the Act.

10.1. Purpose of the Processing of Personal Information

10.1.1 HR

To enable the Company to maintain appropriate human resources records in relation to members of staff, including recruitment and selection, administration of payroll, expenses, accounts, tax, travel and benefits, work management, professional development and performance reviews, discipline, and superannuation. To enable the Company to operate a workplace whistleblowing hotline to detect and prevent improper workplace conduct and crime prevention in accordance with relevant business conduct policies.

10.1.2 Customer Marketing

To enable the Company to maintain a customer relationship marketing database of individuals to whom information and promotional material may be sent in relation to products and services that may be of interest to them.

10.1.3 Customer Care

To enable consumer care via call centres to be provided including integrating external and internal management consumer information across the Reckitt Benckiser Group, embracing finance, manufacturing, sales, and procurement.

10.1.4 IT Administration

To enable IT administration to manage users of the Company network, allowing staff secure access to their IT systems, backing up information on the Company's network, document management, email system (Microsoft Exchange) and intranet service.

10.1.5 Accounts and Records Procurement

To enable procurement of goods and services by the Company

10.1.6 Crime Prevention and Prosecution of Offenders

To enable the prevention and detection of a crime or alleged crime through the use of CCTV on the Company sites.

10.2. Categories of Data Subjects and Personal Information/special Personal Information relating thereto.

As per section 1 of POPIA, a data subject may either be a natural or a juristic person. The categories of data subjects in respect of which the Companies process Personal Information and the types of Personal Information relating thereto has been set out in detail as per the Annexure hereto titled “Categories of Data Subject and Data”.

10.2.1 HR

The personal data will include:

(i) names and contact details of the data subject;

(ii) employment details;

(iii) financial details;

(iv) educational experience, business activities and skill set;

(v) family members (where provided as point of contact); in Mexico

(vi) social activities, hobbies (as cultural, sports, professional, civic), family information.

10.2.2 Customer Marketing

The personal data will include

(i) names and contact details of the data subject including email and telephone details;

(ii) country of residence;

(iii) nationality;

(iv) goods or services provided.

10.2.3 Customer Care

The personal data will include

(i) names and contact details of the data subject;

(ii) employment details;

(iii) financial details;

(iv) (educational experience, business activities and skill set;

(v) family members (where provided as point of contact);

(vi) goods or services provided.

10.2.4 IT Administration

The personal data will include

(i) names and contact details of the data subject;

(ii) employment details;

(iii) family members (where provided as point of contact).

10.2.5 Accounts and Records Procurement

The personal data will include

(i) names and contact details of the data subject;

(ii) employment details;

(iii) goods or services provided

10.2.6 Crime Prevention and Prosecution of Offenders

The personal data will include images of the data subject.

10.3. Recipients or categories of recipients of Personal Information to whom Personal Information may be supplied

10.3.1. The Companies may provide a data subject's Personal Information to recipients to which disclosure is required for regulatory compliance or otherwise as provided for within the provisions of the act, with reference to "processing'':

'Section 1: "processing'' means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(i) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;

(ii) dissemination by means of transmission, distribution or making available in any other form; or

(iii) merging, linking, as well as restriction, degradation, erasure or destruction of information;"

10.3.2. The Companies will not without grounds for lawful processing, disclose personal information of the data subject in contravention of the data subject's right to privacy.

10.4. Planned Transborder flow of Personal Information

Any international data transfers will be within the Company, with confidentiality provisions being imposed and within the strict operation of intra-group data transfer agreements, ensuring the protection of data subjects' rights and adherence to regulatory provisions.

10.5. Description of the information security measures to be implemented by the Companies to ensure the confidentiality, integrity and availability of the information which is to be processed –

The Company is committed to safeguarding the security of all personal data which it processes through day-to-day operations. To achieve this, the Company has developed and implemented technical and organisational measures that strive to safeguard this important asset. The measures form a robust Information Security protection program made up of data privacy and security policies and functional specific Standard Operating Procedures, which include the following measures:

10.5.1 Information Security Policies and Standards

Implement security requirements within the organisation and for staff and all Sub processors, service providers, or agents who have access to Personal Data to maintain the integrity, confidentiality, resilience, and availability of Personal Data, to include (but not be limited to) the following:

(i) Prevent unauthorized persons from gaining access to Personal Data processing systems (physical access control);

(ii) Prevent Personal Data processing systems being used without authorization (logical access control);

(iii) Ensure that persons entitled to use a Personal Data processing system gain access only to such Personal Data as they are entitled to access in accordance with their access rights and that, while Processing or use and after storage, Personal Data cannot be read, copied, modified, or deleted without authorization (data access control);

(iv) Ensure that Personal Data cannot be read, copied, modified, or deleted without authorization during electronic transmission, transport, or storage, and that the target entities for any transfer

of Personal Data by means of data transmission facilities can be established and verified, with appropriate pseudonymization and encryption measures adopted to protect the confidentiality of data during transfer and storage (data transfer and storage control);

(v) Ensure the establishment of an audit trail to document whether and by whom Personal Data have been entered into, modified in, or removed from Personal Data Processing (entry control);

(vi) Ensure that Personal Data are Processed solely in accordance with the processor's Instructions (control of instructions);

(vii) Ensure that Personal Data are protected against accidental destruction or loss, and appropriate measures adopted to support access to data and / or restoration of data in the event of a physical or technical incident impacting availability (availability control); and

(viii) Ensure that Personal Data collected for different purposes can be processed separately (separation control).

These rules shall be kept up to date and revised whenever relevant changes are made to any information system that uses or houses Personal Data, or to how that system is organised.

These rules shall be routinely reviewed to evaluate efficacy and areas for improvement and where relevant adopt and apply changes as part of a continuous improvement programme.

10.5.2 Physical Security

The transferee / data importer will maintain commercially reasonable security systems at all transferee / data importer sites at which an information system that uses or houses Personal Data is located. The Suppler reasonably and appropriately restrict access to such Personal Data. Physical access control shall be implemented for all data centres. Unauthorised access is prohibited through 24x7 onsite staff and security camera monitoring.

10.5.3 Organisational Security transferee / data importer shall ensure that it has implemented security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees.

10.5.4 All Personal Data security incidents shall be managed in accordance with appropriate incident response procedures.

10.5.5 Network Security

The transferee / data importer shall maintain network security using commercially available equipment and industry standard techniques, including firewalls, intrusion detection systems, ccess control lists and routing protocols.

10.5.6 Access Control

(i) Only authorised staff shall be permitted to grant, modify, or revoke access to an information system that uses or houses Personal Data.

(ii) User administration procedures shall be adopted which define user roles and their privileges, how access is granted, changed, and terminated; addresses appropriate segregation of duties; and defines the logging/monitoring requirements and mechanisms.

(iii) All employees of the transferee / data importer shall be assigned unique User-IDs.

(iv) Access rights shall be implemented adhering to the "least privilege" approach.

(v) The transferee / data importer shall implement commercially reasonable physical and electronic security to create and protect passwords.

11. VIRUS AND MALWARE CONTROLS

The transferee / data importer shall install and maintain industry standard (which shall comprise the latest version) anti-virus and malware protection software on the system.

12. PERSONNEL

12.1. The transferee / data importer shall implement a security awareness program to train personnel about their security obligations. This program shall include training about data classification obligations, physical security controls, security practices and security incident reporting.

12.2. The transferee / data importer shall have clearly defined roles and responsibilities for its employees. Screening is implemented before employment with terms and conditions of employment applied appropriately.

12.3. The transferee / data importer personnel shall strictly follow established security policies and procedures. Disciplinary process will be appropriately applied if employees commit a security breach.

13. ADDITIONAL SECURITY REQUIREMENTS

13.1. The transferee / data importer shall not delete or remove any proprietary notices contained within or relating to Personal Data.

13.2. The transferee / data importer shall perform and maintain secure back-ups of all Personal Data and shall ensure that up-to-date back-ups are stored off-site. transferee / data importer shall ensure that such back-ups are available to transferor / data exporter (or to such other person as transferor / data exporter may direct) at no additional cost to transferor / data exporter, and that the data contained in the back-ups are available at all times upon request and are delivered to transferor / data exporter at no less than six (6) monthly intervals (or such other intervals as may be agreed in writing between the Parties).

13.3. The transferee / data importer shall ensure that any system on which it holds any Personal Data, including back-up data, is a secure system that complies with all security requirements.

13.4. If Personal Data is corrupted, lost or sufficiently degraded as a result of the transferee / data importer 's default so as to be unusable, transferor / data exporter may:

13.4.1. require the transferee / data importer (at the transferee / data importer's expense) to restore or procure the restoration of Personal Data to the extent possible and transferee / data importer shall do so as soon as practicable but not later than five (5) days from the date of receipt of TRANSFEROR / DATA EXPORTER's notice; and/or

13.4.2. itself restore or procure the restoration of Personal Data and shall be repaid by the transferee / data importer any reasonable expenses incurred in doing so.

13.5. If at any time the transferee / data importer suspects or has reason to believe that Personal Data has or may become corrupted, lost, or sufficiently degraded in any way for any reason, then the transferee / data importer shall notify transferor / data exporter immediately and inform transferor / data exporter of the remedial action the transferee / data importer proposes to take.

14. MALICIOUS SOFTWARE

14.1. The transferee / data importer shall, as an enduring obligation and at no cost to

TRANSFEROR / DATA EXPORTER, use the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor (unless otherwise agreed in writing between the Parties) to check for, contain the spread of, and minimise the impact of Malicious Software in the relevant IT environment

(or as otherwise agreed by the Parties). The transferee / data importer may be required to provide details of the version of anti-virus software being used in certain circumstances (e.g., in response to a specific threat).

14.2. Notwithstanding paragraph 14.1, if Malicious Software is found, the Parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Personal Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

14.3. Any cost arising out of the actions of the Parties taken in compliance with the provisions of paragraphs 14.1 and 14.2 shall be borne by the Parties as follows:

14.3.1. by the transferee / data importer where the Malicious Software originates from the transferee / data importer 's software, the third-party software supplied by the transferee / data importer (except where transferor / data exporter has waived the obligation) or Personal Data (whilst such Personal Data was under the control of the transferee / data importer or any of its Sub processors) unless the transferee / data importer can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by transferor / data exporter when provided to the transferee / data importer ; and

14.3.2. Otherwise by transferor / data exporter

15. FORMS

https://www.justice.gov.za/forms/paia/J752_paia_Form%20C.pdf

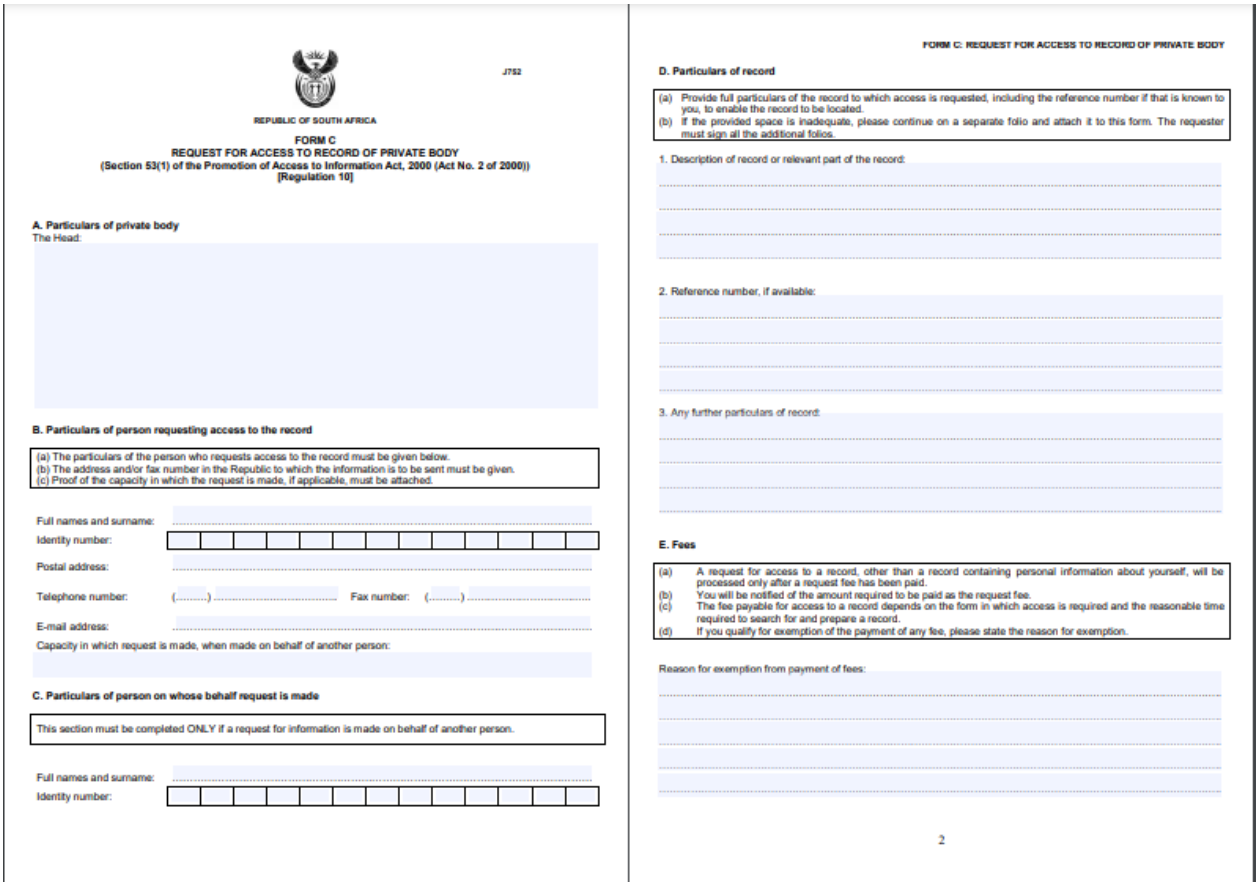
FORM C

REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

(Section 53(1) of the Promotion of Access to Information Act, 2000

(Act No. 2 of 2000))

[Regulation 10]



J752

REPUBLIC OF SOUTH AFRICA

FORM C
REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY
(Section 53(1) of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000))
[Regulation 10]

A. Particulars of private body
The Head:

B. Particulars of person requesting access to the record

(a) The particulars of the person who requests access to the record must be given below.
(b) The address and/or fax number in the Republic to which the information is to be sent must be given.
(c) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:
Identity number:
Postal address:
Telephone number: (.....) Fax number: (.....)
E-mail address:
Capacity in which request is made, when made on behalf of another person:

C. Particulars of person on whose behalf request is made

This section must be completed ONLY if a request for information is made on behalf of another person.

Full names and surname:
Identity number:

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

D. Particulars of record

(a) 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.
(b) If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of record or relevant part of the record:

2. Reference number, if available:

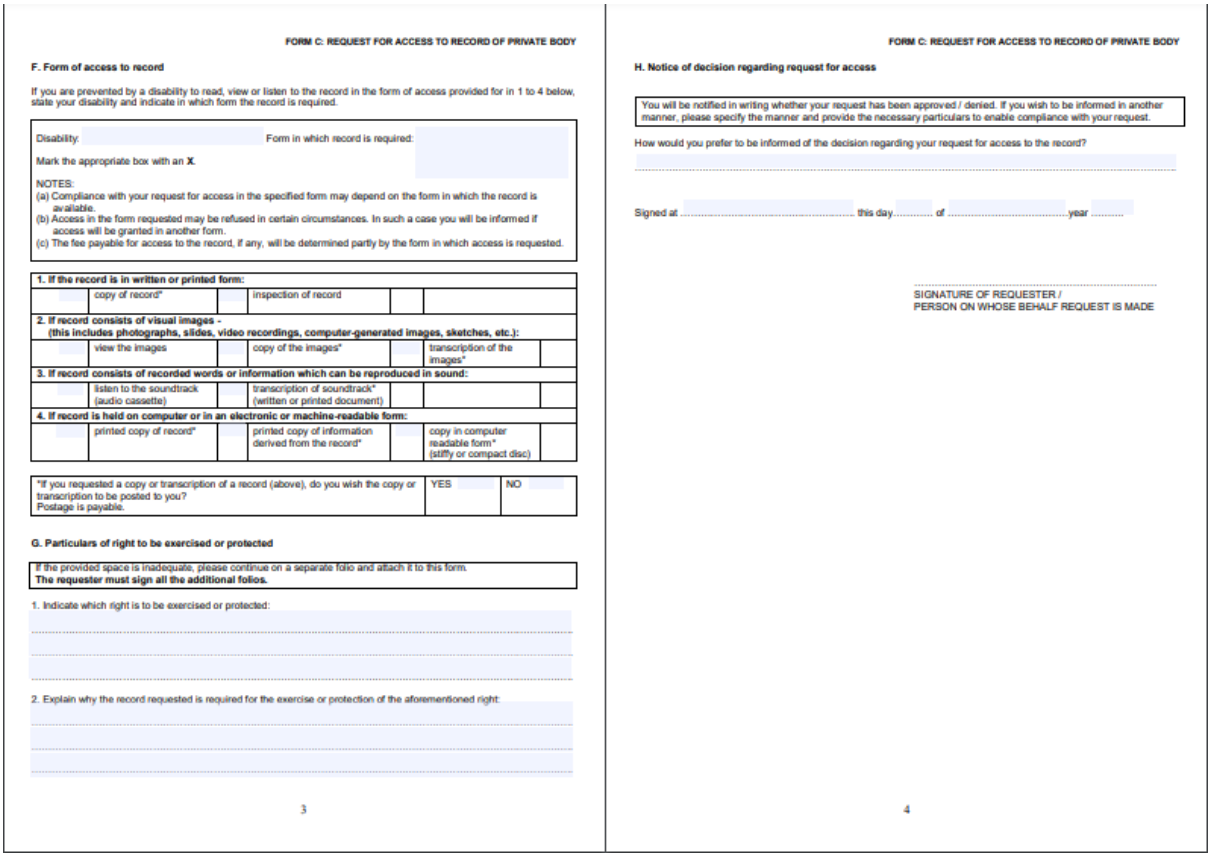
3. Any further particulars of record:

E. Fees

(a) A request for access to a record, other than a record containing personal information about yourself, will be processed only after a request fee has been paid.
(b) You will be notified of the amount required to be paid as the request fee.
(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 for exemption from payment of fees:

2



FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

F. Form of access to record

If you are prevented by a disability to read, view or listen to the record in the form of access provided for in 1 to 4 below, state your disability and indicate in which form the record is required.

Disability: Form in which record is required:

Mark the appropriate box with an **X**.

NOTES:
(a) Compliance with your request for access in the specified form may depend on the form in which the record is available.
(b) Access in the form requested may be refused in certain circumstances. In such a case you will be informed if access will be granted in another form.
(c) The fee payable for access to the record, if any, will be determined partly by the form in which access is requested.

1. If the record is in written or printed form:					
	copy of record*		inspection of record		
2. If record consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):					
	view the images		copy of the images*		transcription of the images*
3. If record consists of recorded words or information which can be reproduced in sound:					
	listen to the soundtrack (audio cassette)		transcription of soundtrack* (written or printed document)		
4. If record is held on computer or in an electronic or machine-readable form:					
	printed copy of record*		printed copy of information derived from the record*		copy in computer readable form* (stiffy or compact disc)

*If you requested a copy or transcription of a record (above), do you wish the copy or transcription to be posted to you? Postage is payable.	YES	NO

G. Particulars of right to be exercised or protected

If the provided space is inadequate, please continue on a separate folio and attach it to this form.
The requester must sign all the additional folios.

1. Indicate which right is to be exercised or protected:

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

3

FORM C: REQUEST FOR ACCESS TO RECORD OF PRIVATE BODY

H. Notice of decision regarding request for access

You will be notified in writing whether your request has been approved / denied. If you wish to be informed in another manner, please specify the manner and provide the necessary particulars to enable compliance with your request.

How would you prefer to be informed of the decision regarding your request for access to the record?

Signed at ..... this day..... of .....year .....

SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MADE

4

SOUTH AFRICAN HUMAN RIGHTS DISCLAIMER

The South African Human Rights Commission reserves all rights and makes no warranty, either express or implied, with respect to the information and/or promotional material contained herein and is not responsible for any expenses, inconvenience, damage (whether special or consequential) or claims arising out of posting, time and costs incurred and or associated with this information and will not be liable for the latter. Specific exemption from any liability is claimed with regard to the following:

- The SAHRC does not endorse any third-party private service provider and will not bear any costs related to your transaction to compile the manual on your behalf.
- Submission to the SAHRC is free and the SAHRC does not charge any fees for advice or administration however all cost to lodge manuals is at the relevant private entities own cost e.g., registered mail etc.
- Manuals are subject to review and comment with the possibility of manuals being rejected on the basis of not meeting the minimum requirements and the SAHRC is not liable for the amendment costs if any and resubmission if any of any manuals.