



G.U.D. Holdings

LEADERS IN AUTOMOTIVE PRODUCTS

G.U.D. HOLDINGS (PROPRIETARY) LIMITED

MANUAL

as prescribed by the provisions of

THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000

And

THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

Contents

1	DEFINITIONS.....	3
2	PURPOSE OF THE MANUAL	4
3	COMPANY DETAILS.....	4
4	CONTACT DETAILS OF THE INFORMATION OFFICER.....	4
5	THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION	4
6	PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA.....	5
7	GROUND FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA.....	5
8	INFORMATION OR RECORDS NOT FOUND	6
9	REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL OF A REQUEST FOR ACCESS IN TERMS OF PAIA	6
10	PROCEDURE FOR A REQUEST FOR ACCESS IN TERMS OF PAIA	6
11	FEES.....	7
12	DECISION TO GRANT ACCESS TO RECORDS	7
13	AVAILABILITY OF THE MANUAL	7
14	PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY THE COMPANY	8
	Appendix 1 - Subsidiaries	10
	Appendix 2 - Categories of records held by the Company	11
	Appendix 3 - Legislation in terms of which records are held by the Company	13
	Appendix 4 - Access Request Form	15
	Appendix 5 - Fees	19
	Appendix 6 - Processing of Personal Information in accordance with POPIA.....	20
	Appendix 7 - Objection to the Processing of Personal information in terms of Section 11(3) of the Protection of personal information	23
	Appendix 8 - 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.....	24
	Appendix 9 - Protection of personal Information Policy.....	26

1 DEFINITIONS

- 1.1 **Company** means G.U.D Holdings (Pty) Ltd (registration number 1949/034522/07), a company duly registered and incorporated with limited liability in accordance with the company laws of the Republic of South Africa and having its principal place of business situated at 3 The Avenue East, Isipingo, Durban KZN, Republic of South Africa together with its subsidiaries as specified in **Appendix 1**;
- 1.2 **Conditions for Lawful Processing** means the conditions for the lawful processing of Personal Information as fully set out in chapter 3 of POPIA;
- 1.3 **Constitution** means the Constitution of the Republic of South Africa, 1996;
- 1.4 **Customer** refers to any natural or juristic person that received or receives services from the Company;
- 1.5 **Data Subject** has the meaning ascribed thereto in section 1 of POPIA;
- 1.6 **Head of the Company** means the “head” as defined in section 1 of PAIA and referred to in clause 4;
- 1.7 **Information Officer** means the Company’s Chief Executive Officer;
- 1.8 **Manual** means this manual prepared in accordance with section 51 of PAIA and regulation 4(1) (d) of the POPIA Regulations;
- 1.9 **PAIA** means the *Promotion of Access to Information Act, 2000*;
- 1.10 **Personal Information** has the meaning ascribed thereto in section 1 of POPIA;
- 1.11 **Personnel** refers to any person who works for, or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Company, which includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff as well as contract workers;
- 1.12 **POPIA** means the *Protection of Personal Information Act, 2013*;
- 1.13 **POPIA Regulations** mean the regulations promulgated in terms of section 112(2) of POPIA;
- 1.14 **Private Body** has the meaning ascribed thereto in sections 1 of both PAIA and POPIA;
- 1.15 **Processing** has the meaning ascribed thereto in section 1 of POPIA;
- 1.16 **Responsible Party** has the meaning ascribed thereto in section 1 of POPIA;
- 1.17 **Record** has the meaning ascribed thereto in section 1 of PAIA and includes Personal Information;
- 1.18 **Requester** has the meaning ascribed thereto in section 1 of PAIA;
- 1.19 **Request for Access** has the meaning ascribed thereto in section 1 of PAIA; and
- 1.20 **SAHRC** means the South African Human Rights Commission.

Capitalised terms used in this Manual have the meanings ascribed thereto in section 1 of POPIA and PAIA as the context specifically requires, unless otherwise defined herein.

2 PURPOSE OF THE MANUAL

This Manual:

- 2.1 for the purposes of PAIA, details the procedure to be followed by a Requester and the manner in which a Request for Access will be facilitated; and
- 2.2 for the purposes of POPIA, amongst other things, details the purpose for which Personal Information may be processed; a description of the categories of Data Subjects for whom the Company 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.

3 COMPANY DETAILS

- 3.1 The details of the Company are as follows:

Physical address	3 The Avenue East Isipingo KZN
Postal address:	PO Box 26100 Isipingo Beach 4115
Telephone number:	031 910 3100
Fax number	031 910 3111

4 CONTACT DETAILS OF THE INFORMATION OFFICER

- 4.1 The Information Officer's contact details are as follows:

Physical address	3 The Avenue East Isipingo KZN
Postal address	PO Box 26100 Isipingo Beach 4115
email address:	legal@gud.co.za
Fax number	031 9027797

5 THE SOUTH AFRICAN HUMAN RIGHTS COMMISSION

- 5.1 The SAHRC has compiled a guide, as contemplated in section 10 of the South African Human Rights Commission Act, 2013 ("**the Act**") containing information to assist any person who wishes to exercise any right as contemplated in the Act.
- 5.2 This guide is available from the SAHRC at:

Postal address	Private Bag 2700 Houghton 2041
Website	www.sahrc.org.za
Telephone number	011 877 3600
Fax number	011 403 0684

6 PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA

6.1 Schedule of Records

The Schedule of Records as contained in **Appendix 2** of this Manual details the Records that are held and/or Processed by the Company for the purposes of PAIA and POPIA respectively. Such Access to such Records may not be granted if they are subject to the grounds of refusal which are specified in clause 7 below.

6.2 List of applicable legislation

- (1) The Company retains records which are required in terms of legislation other than PAIA.
- (2) Certain legislation provides that private bodies shall allow certain persons access to specified records, upon request. Legislation that may be consulted to establish whether the Requester has a right of access to a record other than in terms of the procedure set out in the PAIA are set out in **Appendix 3**.

7 GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA

The following are the grounds on which the Company may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA:

- 7.1 mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of Personal Information would be unreasonable;
- 7.2 mandatory protection of the commercial information of a third party, if the Records contain:
 - (1) trade secrets of that third party;
 - (2) financial, commercial, scientific or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or
 - (3) information disclosed in confidence by a third party to the Company, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition;
- 7.3 mandatory protection of confidential information of third parties if it is protected in terms of any agreement;
- 7.4 mandatory protection of the safety of individuals and the protection of property;
- 7.5 mandatory protection of Records that would be regarded as privileged in legal proceedings;
- 7.6 protection of the commercial information of the Company, which may include:
 - (1) trade secrets;
 - (2) financial/commercial, scientific or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of the Company;

- (3) information which, if disclosed, could put the Company at a disadvantage in contractual or other negotiations or prejudice the Company in commercial competition; and/or
- (4) computer programs which are owned by the Company, and which are protected by copyright and intellectual property laws;

7.7 research information of the Company or a third party, if such disclosure would place the research or the researcher at a serious disadvantage; and

7.8 Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

8 INFORMATION OR RECORDS NOT FOUND

If the Company cannot find the records that the Requester is looking for despite reasonable and diligent search and it believes either that the records are lost or that the records are in its possession but unattainable, the Requester will receive a notice in this regard from the Information Officer in the form of an affidavit setting out the measures taken to locate the document and accordingly the inability to locate the document.

9 REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL OF A REQUEST FOR ACCESS IN TERMS OF PAIA

9.1 The Company does not have internal appeal procedures. As such, the decision made by the Information Officer is final, and Requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.

9.2 In accordance with sections 56(3) (c) and 78 of PAIA, a Requester may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

10 PROCEDURE FOR A REQUEST FOR ACCESS IN TERMS OF PAIA

10.1 A Requester must comply with all the procedural requirements as contained in section 53 of PAIA relating to a Request for Access to a Record.

10.2 A Requester must complete the prescribed Request for Access form attached as **Appendix 4**, and submit the completed Request for Access form as well as payment of a request fee (if applicable) and a deposit (if applicable), to the Information Officer at the postal or physical address, facsimile number or electronic mail address stated in clause 4 above.

10.3 The Request for Access form must be completed with enough detail so as to enable the Information Officer to identify the following:

- (1) the Record/s requested;
- (2) the identity of the Requester;
- (3) the form of access that is required, if the request is granted;
- (4) the postal address or fax number of the Requester; and
- (5) the right that the Requester is seeking to protect and an explanation as to why the Record is necessary to exercise or protect such a right.

10.4 If a Request for Access is made on behalf of another person, the Requester must submit proof of the capacity in which the Requester is making the request to the reasonable satisfaction of the Information Officer.

10.5 If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally.

10.6 The Company will voluntarily provide the requested Records to a Personal Requester (as defined in section 1 of PAIA). The prescribed fee for reproduction of the Record requested by a Personal Requester will be charged in accordance with section 54(6) of PAIA and paragraph 11 below.

11 FEES

11.1 When the Request for Access is received by the Information Officer, the Information Officer will by notice require the Requester, other than a Personal Requester, to pay the prescribed request fee (if any), before further processing of the Request for Access.

11.2 Prescribed request fees are set out in **Appendix 5**.

11.3 If the search for a Record requires more than the prescribed hours for this purpose, the Information Officer will notify the Requester to pay as a deposit, the prescribed portion of the access fee (being not more than one third) which would be payable if the Request for Access is granted.

11.4 The Information Officer will withhold a Record until the Requester has paid the fees set out in **Appendix 5**.

11.5 A Requester whose Request for Access to a Record has been granted, must pay an access fee for reproduction and for search and preparation, and for any time reasonably required in excess of the prescribed hours to search for and prepare the Record for disclosure, including making arrangements to make it available in a requested form provided for in PAIA.

11.6 If a deposit has been paid in respect of a Request for Access which is refused, the Information Officer will repay the deposit to the Requester.

12 DECISION TO GRANT ACCESS TO RECORDS

12.1 The Company will decide whether to grant or decline the Request for Access within 30 days of receipt of the Request for Access and must give notice to the Requester with reasons (if required) to that effect.

12.2 The period referred to above may be extended for a further period of not more than 30 days if the Request for Access is for a large number of Records or the Request for Access requires a search for Records held at another office of the Company and the Records cannot reasonably be obtained within the original 30 day period.

12.3 The Company will notify the Requester in writing should an extension of time as contemplated above be required.

12.4 If, in addition to a written reply from the Information Officer, the Requester wishes to be informed of the decision on the Request for Access in any other manner, the Requester must state the manner and particulars so required.

13 AVAILABILITY OF THE MANUAL

13.1 This Manual is made available in terms of PAIA and section 4 of the Regulations to POPIA.

13.2 This Manual is also available at: www.gudholdings.co.za

13.3 This Manual is further available at the offices of SAHRC and at the offices of the Company for inspection during normal business hours. No fee will be levied for inspection as contemplated in this clause.

13.4 Copies of the Manual can be obtained from the Information Officer. A fee will be levied for copies of the manual in accordance with **Appendix 5**.

14 PROTECTION OF PERSONAL INFORMATION THAT IS PROCESSED BY THE COMPANY

14.1 Chapter 3 of POPIA provides for the minimum Conditions for Lawful Processing of Personal Information by a Responsible Party.

14.2 The Company needs Personal Information relating to both individual and juristic persons in order to carry out its business and organisational functions. The manner in which this information is Processed and the purpose for which it is Processed is determined by the Company. The Company is accordingly a Responsible Party for the purposes of POPIA and will ensure that the Personal Information of a Data Subject:

- (1) is processed lawfully, fairly and transparently. This includes the provision of appropriate information to Data Subjects when their data is collected by the Company, in the form of privacy or data collection notices. The Company must also have a legal basis (for example, consent) to process Personal Information;
- (2) is processed only for the purposes for which it was collected;
- (3) will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
- (4) is adequate, relevant and not excessive for the purposes for which it was collected;
- (5) is accurate and kept up to date;
- (6) will not be kept for longer than necessary;
- (7) is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that Personal Information, in both physical and electronic form, are subject to an appropriate level of security when stored, used and communicated by the Company, in order to protect against access and acquisition by unauthorised persons and accidental loss, destruction or damage;
- (8) is processed in accordance with the rights of Data Subjects, where applicable. Data Subjects have the right to:
 - (a) be notified that their Personal Information is being collected by the Company. The Data Subject also has the right to be notified in the event of a data breach;
 - (b) know whether the Company holds Personal Information about them, and to access that information. Any request for information must be handled in accordance with the provisions of this Manual;
 - (c) request the correction or deletion of inaccurate, irrelevant, excessive, out of date, incomplete, misleading or unlawfully obtained personal information;
 - (d) object to the Company's use of their Personal Information and request the deletion of such Personal Information (deletion would be subject to the Company's recordkeeping requirements);
 - (e) object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications; and
 - (f) complain to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.

14.3 Purpose of the Processing of Personal Information by the Company

Part 1 of Appendix 6 sets out purposes for which the Company Processes or will Process Personal Information.

14.4 Categories of Data Subjects and Personal Information/special Personal Information relating thereto

Part 2 of Appendix 6 sets out the various categories of Data Subjects that the Company Processes Personal Information on and the types of Personal Information relating thereto.

14.5 Recipients of Personal Information

Part 3 of Appendix 6 outlines the recipients to whom the Company may provide a Data Subjects Personal Information to.

14.6 Cross-border flows of Personal Information

Section 72 of POPIA provides that Personal Information may only be transferred out of the Republic of South Africa if the:

- 14.6.A recipient country can offer such data an “adequate level” of protection. This means that data privacy laws must be substantially similar to the Conditions for Lawful Processing as contained in POPIA; or
- 14.6.B Data Subject consents to the transfer of their Personal Information; or
- 14.6.C transfer is necessary for the performance of a contractual obligation between the Data Subject and the Responsible Party; or
- 14.6.D transfer is necessary for the performance of a contractual obligation between the Responsible Party and a third party, in the interests of the Data Subject; or
- 14.6.E the transfer is for the benefit of the Data Subject, and it is not reasonably practicable to obtain the consent of the Data Subject, and if it were, the Data Subject, would in all likelihood provide such consent.

Part 4 of Appendix 6 sets out the planned cross-border transfers of Personal Information and the condition from above that applies thereto.

14.7 Description of information security measures to be implemented by the Company

Part 5 of Appendix 6 sets out the types of security measures to implemented by the Company in order to ensure that Personal Information is respected and protected.

14.8 Objection to the Processing of Personal Information by a Data Subject

Section 11 (3) of POPIA and regulation 2 of the POPIA Regulations provides that a Data Subject may, at any time object to the Processing of his/her/its Personal Information in the prescribed form attached to this manual as **Appendix 7** subject to exceptions contained in POPIA.

14.9 Request for correction or deletion of Personal Information

Section 24 of POPIA and regulation 3 of the POPIA Regulations provides that a Data Subject may request for their Personal Information to be corrected/deleted in the prescribed form attached as **Appendix 8** to this Manual.

14.10 Protection of Personal Information Policy

A copy of the Company’s Protection of Personal Information Policy is attached as **Appendix 9**.

SUBSIDIARIES

1	G.U.D. Africa (Pty) Ltd
2	GUD Autodetox (Pty) Ltd
3	G.U.D. Atlantis (Pty) Ltd
4	Indy Oil SA (Pty) Ltd
5	Safeline Brakes (Pty) Ltd
6	O Muller Property Development (Pty) Ltd
7	ECE 90 Brake Testing (Pty) Ltd
8	Precision Press (Pty) Ltd
9	G.U.D. Chemicals (Pty) Ltd

Appendix 2
Categories of records held by the Company

Records	Subject
Customer Records	<ul style="list-style-type: none"> • Customer correspondence • Customer deal files • Customer agreements • Customer business information • Legal documentation • Proposal and tender documents • Project plans • Risk management records • Standard terms and conditions of supply of goods and/or services • Working papers
Corporate Governance	<ul style="list-style-type: none"> • Board meeting minutes • Codes of conduct • Corporate social investment records • Executive committee meeting minutes • Legal compliance records • Policies
Finance and Administration	<ul style="list-style-type: none"> • Accounting records • Agreements • Annual financial statements • Banking records • Correspondence • Fixed asset register • Invoices and statements • Movable Asset Register • Purchase orders • Remittance • Statistics SA returns • Tax records and returns • Legal dispute records
Human Resources	<ul style="list-style-type: none"> • Assessments • BEE statistics • Career development records • Employment equity reports • General terms of employment • Letters of employment • Leave records • Medical records • Occupational health and safety • PAYE records and returns • Performance management records • Personnel information • Policies and procedures • Provident Fund, rules, life and disability records • Skills development levies • Training material • Training records and statistic • Training Agreements • UIF returns

Information Management and Technology	<ul style="list-style-type: none"> • Agreements • Equipment register • Information policies • Licenses • Standards, procedures and guidelines • Software packages
Marketing and Communication	<ul style="list-style-type: none"> • Proposal documents • New business development • Brand information and strategy • Marketing strategies • Communication strategies • Agreements • Customer relationship programmes • Marketing publications and brochures
Operations	<ul style="list-style-type: none"> • Access control records • Agreements • Archived administration documentation • Environmental records • General correspondence • Patents and Trade Mark documents • Insurance documentation • Service level agreements • Standard trading terms and conditions of supply of services and goods • Supplier records and correspondence • Travel documentation; • Procurement agreements and documentation; • Vehicle registration documents; and • Cellular phone registration documents, including RICA.
Secretarial	<p>Applicable statutory document, including but not limited to:</p> <ul style="list-style-type: none"> • Certificates of Incorporation and certificates to commence business • Corporate structure documents • Memoranda and Articles of Association • Share registers • Statutory Returns to relevant authorities • Share certificates • Minutes of meetings • Resolutions passed • Director appointments and resignations

Appendix 3
Legislation in terms of which records are held by the Company

1.	No 46 of 1998	Administration of Adjudication of Road Traffic Offences Act
2.	No 66 of 1965	Administration of Estates Act
3.	No 21 of 1940	Advertising on Roads & Ribbon Development Act
4.	No 75 of 1997	Basic Conditions of Employment Act
5.	No 34 of 1964	Bills of Exchange Act
6.	No 53 of 2003	Broad-Based Black Economic Empowerment Act
7.	No 4 of 1999	Broadcasting Act
8.	No 69 of 1984	Close Corporations Act
9.	No 71 of 2008	Companies Act
10.	No 130 of 1993	Compensation for Occupational Injuries and Diseases Act
11.	No 89 of 1998	Competition Act
12.	No 108 of 1996	Constitution of South Africa Act
13.	No 68 of 2009	Consumer Protection Act
14.	No 98 of 1987	Copyright Act
15.	No 51 of 1977	Criminal Procedure Act
16.	No 9 of 1933	Currency & Exchanges Act
17.	No 91 of 1964	Customs and Excise Act
18.	No 70 of 1979	Divorce Act
19.	No 36 of 2005	Electronic Communications Act
20.	No 25 of 2002	Electronic Communications and Transactions Act
21.	No 55 of 1998	Employment Equity Act
22.	No 73 of 1989	Environment Conservation Act
23.	No 37 of 2002	Financial Advisory & Intermediary Services Act
24.	No 38 of 2001	Financial Intelligence Centre Act
25.	No 60 of 2000	Firearms Control Act
26.	No 18 of 1969	Formalities In Respect of Leases of Land Act
27.	No 63 of 1977	Health Act
28.	No 58 of 1962	Income Tax Act
29.	No 66 of 1995	Labour Relations Act
30.	No 52 of 1998	Long Term Insurance Act
31.	No 99 of 1998	Maintenance Act
32.	No 103 of 1997	National Building Regulations and Building Standards Act
33.	No 34 of 2005	National Credit Act
34.	No 107 of 1998	National Environmental Management Act
35.	No 39 of 2004	National Environmental Management: Air Quality Act
36.	No 59 of 2008	National Environmental Management: Waste Act
37.	No 36 of 1998	National Water Act
38.	No 93 of 1996	National Road Traffic Act
39.	No 85 of 1993	Occupational Health and Safety Act
40.	No 57 of 1987	Patents Act
41.	No 24 of 1956	Pension Funds Act
42.	No 18 of 1943	Prescription Act
43.	No 12 of 2004	Prevention & Combating of Corrupt Activities Act
44.	No 33 of 2004	Prevention of Constitutional Democracy Against Terrorist & Related Activities Act
45.	No 121 of 1998	Prevention of Organised Crime Act
46.	No 2 of 2000	Promotion of Access to Information Act

47.	No 4 of 2000	Promotion of Equality and Prevention of Unfair Discrimination Act
48.	No 26 of 2000	Protected Disclosures Act 26 of 2000
49.	No 70 of 2002	Regulation of Interception of Communications and Provisions of Information Act
50.	No 25 of 1964	Sales and Service Matters Act
51.	No 23 of 1955	Second-Hand Goods Act
52.	No 95 of 1986	Sectional Titles Act
53.	No 36 of 2004	Securities Services Act
54.	No 25 of 2007	Securities Transfer Act
55.	No 53 of 1998	Short-Term Insurance Act
56.	No 97 of 1997	Skills Development Act
57.	No 9 of 1999	Skills Development Levies Act
58.	No 90 of 1989	South African Reserve Bank Act
59.	No 57 of 1988	Trust Property Control Act
60.	No 7 of 1998	The South African National Roads Agency Limited & National Roads Act
61.	No 12 of 1999	Tobacco Products Control Act
62.	No 194 of 1993	Trade Marks Act
63.	No 40 of 1949	Transfer Duty Act
64.	No 63 of 2001	Unemployment Insurance Act
65.	No 4 of 2002	Unemployment Insurance Fund Contributions Act
66.	No 89 of 1991	Value-Added Tax Act

The content and extent of this list may be extended from time to time.



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

Designation
E-Mail Address
Physical Address
Telephone number

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:

--	--	--	--	--	--	--	--	--	--	--	--

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:

.....
.....
.....
.....

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 of record:
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:

.....
.....
.....

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..... ofyear

.....
SIGNATURE OF REQUESTER /
PERSON ON WHOSE BEHALF REQUEST IS MA

FEES

1 The fee for a copy of the manual as contemplated in regulation 9(2)(c) is R1,10 for every photocopy of an A4-size page or part thereof.

2 The fees for reproduction referred to in regulation 11(1) are as follows:

			R
(a)		For every photocopy of an A4-size page or part thereof	1,10
(b)		For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
(c)		For a copy in a computer-readable form on -	
(d)	(i)	For a transcription of visual images, for an A4-size page or part thereof	40,00
	(ii)	For a copy of visual images	60,00
(e)	(i)	For a transcription of an audio record, for an A4-size page or part thereof	20,00
	(ii)	For a copy of an audio record	30,00

3 The request fee payable by a requester, other than a personal requester, referred to in regulation 11(2) is R50,00.

4 The access fees payable by a requester referred to in regulation 11(3) are as follows:

			R
(1)	(a)	For every photocopy of an A4-size page or part thereof	1,10
	(b)	For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine readable form	0,75
	(c)	For a copy in a computer-readable form on -	
	(d)	(i) For a transcription of visual images, for an A4-size page or part thereof	40,00
		(ii) For a copy of visual images	60,00
	(e)	(i) For a transcription of an audio record, for an A4-size page or part thereof	20,00
		(ii) For a copy of an audio record	30,00
	(f)	To search for and prepare the record for disclosure, R30,00 for each hour or part of an hour reasonably required for such search and preparation.	

5 For purposes of section 54(2) of PAIA, the following applies:

5.1 Six hours as the hours to be exceeded before a deposit is payable; and

5.2 one third of the access fee is payable as a deposit by the requester.

6 The actual postage is payable when a copy of a record must be posted to a requester.

Part 1

PROCESSING OF PERSONAL INFORMATION IN ACCORDANCE WITH POPIA

Purpose of the Processing of Personal Information	Type of Processing
<ul style="list-style-type: none"> ▪ Operating our business; ▪ To provide goods and services to you in accordance with our agreed terms and to manage the Company's relationship with you; ▪ Analysis, evaluation, review and collation of information in order to determine sales issues and potential disputes, provide sales advice and prepare or comment on sales issues or service opinions, agreements, correspondence, reports, publications, documents relating to projects and other documents and records (whether in electronic or any other medium whatsoever); ▪ Compliance with applicable law, crime detection, prevention, investigation and prosecution; ▪ Transfer of information to any third party providers of various services whom we engage, including but not limited to, providers of information technology, communication, file storage, data storage, copying, printing, accounting or auditing services, experts, insurers and professional advisors and other third parties; ▪ To verify the identity of any representative who contacts the Company on your behalf or who may be contacted by the Company; ▪ For risk assessment, information security management, statistical, trend analysis and planning purposes; ▪ To monitor and record calls and electronic communications with you for quality, training, investigation and fraud prevention purposes; ▪ To enforce or defend the Company's rights; or ▪ Recruitment. 	<ul style="list-style-type: none"> • Collection, • recording, • organization, • structuring, • storage, • adaptation or alteration, • retrieval, • consultation, • use, • disclosure by transmission, • dissemination or otherwise making available, • alignment or combination, • restriction, • erasure or • destruction.

Part 2

Categories of Personal Information that may be processed

Subject	Type of Personal Information	Reason for Collection
Customers	Physical address, name, email, telephone number, change of ownership, identity numbers, Company registration Numbers, credit status, sales volume pricing, VAT Registration/	Maintain customer accounts, understand and agree pricing and demand, manage credit granted
Service Providers	Physical address, name, email, telephone number, change of ownership, identity numbers, Company registration Numbers, BBBEE status, credit status, product pricing and specifications pricing, bank account details, VAT registration.	Maintain service provider records, understand pricing and service offering, pay invoices, understand BBBEE status for BBEEE reporting.
Supplier	Physical address, name, email, telephone number, change of ownership, identity numbers, Company registration Numbers, BBBEE status, credit status, product pricing and specifications pricing, bank account details, VAT registration.	Maintain supplier records, understand supplier pricing and product offering, pay invoices, understand BBBEE status for BBEEE reporting.
Employees	Name, identity number, bank account details, telephone number and address, health, biometrics, race, qualifications.	Maintain accurate records of Employees; to pay salaries, benefits and contributions; for access control and security, complete employment equity returns, qualifications for employment purposes.
Visitors	Name, telephone number, identity number, driver's license,	to maintain occupational health and safety, access security.
Third party contractors	Name, identity number, company name and registration, VAT registration, company address, email, telephone number.	enforce code of; occupational health and safety compliance,

Part 3

Recipients of Personal Information

The Company, its affiliates and their respective representatives

Part 4

Cross border transfers of Personal Information

When making authorized disclosures or transfers of personal information in terms of section 72 of POPIA, Personal Data may be disclosed to recipients located in countries which do not offer a level of protection for those data as high as the level of protection as South Africa.

Part 5

Description of information security measures

The Company undertakes to institute and maintain the data protection measures to accomplish the following objectives outlined below.

Examples of the measure include, but are not limited to, the following:

1	Access Control of Persons The Company shall implement suitable measures in order to prevent unauthorized persons from gaining access to the data processing equipment where the data are processed.
2	Data Media Control The Company undertakes to implement suitable measures to prevent the unauthorized manipulation of media, including reading, copying, alteration or removal of the data media used by the Company and containing personal data of Customers.
3	Data Memory Control The Company undertakes to implement suitable measures to prevent unauthorized input into data memory and the unauthorized reading, alteration or deletion of stored data.
4	User Control The Company shall implement suitable measures to prevent its data processing systems from being used by unauthorized persons by means of data transmission equipment.
5	Access Control to Data The Company represents that the persons entitled to use the Company's data processing system are only able to access the data within the scope and to the extent covered by their respective access permissions (authorization).
6	Transmission Control The Company shall be obliged to enable the verification and tracing of the locations / destinations to which the personal information is transferred by utilization of the Company's data communication equipment / devices.
7	Transport Control The Company shall implement suitable measures to prevent Personal Information from being read, copied, altered or deleted by unauthorized persons during the transmission thereof or during the transport of the data media.
8	Organization Control The Company shall maintain its internal organization in a manner that meets the requirements of this Manual.

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

Note:

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

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)

Signed at this day of20.....

.....

Signature of data subject/designated person

**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**

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018

[Regulation 3]

Note:

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

Mark the appropriate box with an "x".

Request for:

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

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

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/ registered name of data subject:	
Residential, postal or business address:	
Contact number(s):	
Fax number / E-mail address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)

D	REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN. (Please provide detailed reasons for the request)

PROTECTION OF PERSONAL INFORMATION POLICY

1. **INTRODUCTION**

- 1.1 In order for the Company to carry out its objectives as a manufacturer, marketer and Distributor of Automotive, Heavy Duty and industrial products, the Company receives and processes Personal Information.
- 1.2 The Promotion of Access to Information Act of 2000 (“PAIA”) and Protection of Personal Information Act of 2013 (“POPIA”) provides that everyone has the right to the lawful collection, retention, dissemination and use of one’s personal information.
- 1.3 This Policy must be read in conjunction with the Company’s Manual in accordance with PAIA and POPIA available on the Company’s website at www.gudholdings.co.za.

2. **SCOPE AND APPLICATION**

- 2.1. This Policy applies to all Personal Information Processed by the Company, including that information processed by service providers on its behalf, irrespective of whether the Personal Information is stored electronically or on paper.

3. **RESPONSIBLE PARTIES**

- 3.1. The Company undertakes to protect Personal Information and only process Data Subject Personal Information in accordance with POPIA and this Policy.
- 3.2. All customer, suppliers, service providers and Employees acting as Responsible Parties or Operators shall be responsible for safeguarding, protecting and avoiding any unauthorised disclosure of Personal Information in the execution of their contracts with the Company.

4. **LAWFUL PURPOSE**

- 4.1. The Company will ensure that all Personal Information is collected on one of the following grounds:
 - With the consent of the person; or
 - Where it is needed by the Company to perform it’s obligations in terms of a contract; or
 - where required by law; or
 - where the Company has a legitimate interest in collecting the Personal Information.
- 4.2. Where Consent is given to collect Personal Information:
 - 4.2.1. A record of consent will be kept by the Company; and
 - 4.2.2. The consent form must inform the person of the following:

- (a) The type of Personal Information being collected, and if not from the individual then the source from which it is collected
(i.e. credit reports, police clearance, law enforcement databases);
- (b) the name and address of the Company;
- (c) the purpose of collection;
- (d) whether the supply of the Personal Information is voluntary or mandatory;
- (e) any consequences of failing to provide such Personal Information;
- (f) if the Personal Information is to be shared with a third party;
- (g) any other relevant information.

4.3. Where communications are sent to individuals based on their Consent, the individual should be able to easily withdraw their consent.

5. **STRICTLY NECESSARY INFORMATION ONLY**

- 5.1. The Company shall only collect Personal Information needed to perform its activities.
- 5.2. The Company shall contractually require service providers to only collect the Personal Information that is strictly needed to perform their obligations for, or on behalf of the Company.
- 5.3. The Company should take reasonable steps to understand what Personal Information is being collected by service providers, and why such Personal Information is needed to perform their obligations to the Company.
- 5.4. Should the Company find that unnecessary Personal Information is being collected by service providers, the Company must instruct the service provider to destroy or anonymise such information, and to stop from collecting such unnecessary information in future.

6. **KEEPING INFORMATION ACCURATE**

- 6.1. The Company shall take all reasonable steps to ensure Personal Information is kept accurate and up to date.
- 6.2. The Company shall satisfy itself that service providers, who Process Personal Information on its behalf, have reasonable measures in place to keep the Company's Personal Information up to date.
- 6.3. Personal Information must be held in as few places as necessary. Employees of the Company are prohibited from creating any unnecessary additional databases or lists with Personal Information concerning the Company.

7. **ARCHIVING AND RETENTION OF INFORMATION**

- 7.1. The Company shall ensure that service providers have a process of identifying Company records that have met their required retention periods.
- 7.2. Personal Information must generally not be retained for longer than necessary, but this will depend on the importance of the Personal Information.
- 7.3. The Company's general record retention period shall be 5 (five) years after the relevant contract or transaction comes to an end, whereafter such files shall be destroyed.
- 7.4. **Annexure "A"** sets out the retention periods prescribed by law which must be followed by the Company and service providers when Processing the Company's Personal Information.
- 7.5. Documents that are required by law to be kept for certain periods of time shall be stored in a manner and place that is secure.
 - 7.5.1. hardcopy files shall be securely stored in locked cabinets.
 - 7.5.2. digital records shall be stored on a secure server or cloud-storage with access limited to Employees.
- 7.6. The Information Officer shall ensure that a system is developed by the Company whereby documents are archived.
- 7.7. The Information Officer shall ensure that employees are aware of:
 - 7.7.1. where such documents are archived;
 - 7.7.2. who is responsible for their archiving;
 - 7.7.3. who is responsible for destroying such records once their retention period has expired.

8. **DESTRUCTION OF PERSONAL INFORMATION**

- 8.1. The Information Officer is responsible for the continuing process of confirming the destruction of unnecessary and obsolete records containing Personal Information.
- 8.2. The Information Officer shall ensure that service providers have reasonable measures in place to securely destroy Personal Information held on behalf of the Company:
- 8.3. All unwanted paper records containing Personal Information must be shredded before being recycled or disposed of.

9. **INFORMATION PROTECTION RULES**

- 9.1. Data protection rules are risk-based and may be adjusted or changed at any time by the Information Officer whether verbally or otherwise for a particular Employee or service provider to ensure responsive and efficient management of the Company and its risks. As a result, not all data protection rules may be captured in writing.
- 9.2. The Company shall implement, among others, the following technical and organisational security measures to protect Personal Information:

Third party service providers

- 9.2.1. The Company shall enter written “**Operator Agreements**” (data processing agreements) with all service providers that Process Personal Information on behalf of the Company.
- 9.2.2. Operator Agreements must require that service providers:
- (a) are authorised to Process Personal Information on behalf of the Company;
 - (b) are obliged to treat all Personal Information as confidential;
 - (c) set out the reasons why the service provider will Process Personal Information on behalf of the Company;
 - (d) maintain reasonable data protection measures and policies concerning the Company's Personal Information with a similar or higher level of protection to this Policy depending on the nature of the services provided and the importance of the Personal Information Processed by them;
 - (e) provide the Company with a right to audit or inspect the service provider's data protection measures, policies and practices;
 - (f) oblige the service provider to notify the Company of any suspected or actual data breach experienced by the service provider.
- 9.2.3. Before entering into an agreement or sharing any Personal Information with any service provider, and periodically afterwards:
- (a) The Company (either solely or with the assistance legal counsel or external service providers) shall review its service providers who Process Personal Information on its behalf by:
 - (1) Requesting and reviewing a copy of their latest Operator Agreement;
 - (2) Requesting and reviewing a copy of their latest data protection policies, standards or measures;

- (3) Considering any risk of unauthorised disclosure associated with that particular service provider;
- (4) Confirming whether that service provider is authorised to share any Personal Information with any third parties, both within and outside of South Africa and any understanding any risks associated with that sharing of information.

Termination of relationship

- 9.2.4. Employees and service providers must return the Company's information related assets, including but not limited to databases, files, software assets, and equipment (if any), on termination of their employment or services agreement, unless specifically provided for in the relevant agreement. These must be returned before the last day of employment/contract/office or sooner in the event of summary termination.

Technical security measures

- 9.2.5. Employees shall ensure that no Personal Information is stored on their personal computers. Where employees keep or have access to digital records containing Personal Information, such records shall be stored on a secure server or cloud service with:
- (a) password protection;
 - (b) access limited to active Trustees;
 - (c) data centres located in South Africa.
- 9.2.6. Where Employees of the Company use email accounts, mobile phones, software, or laptops to communicate with, transfer or access any documents containing Personal Information, these must be secured by passwords and, where feasible, anti-virus protection and encryption.
- 9.2.7. Employees of the Company must use strong passwords that:
- (a) are changed regularly and never shared between Employees;
 - (b) contain special characters and numbers;
 - (c) do not contain the names of the Employee.
- 9.2.8. Where wireless networks (WIFI) are used to Process or share Personal Information, these networks should be protected by appropriate security measures, including passwords and encryption.
- 9.2.9. Where Personal Information is stored on a CD, DVD, USB, or external hard drives, these must at all times be locked away securely when not in immediate use.

- 9.2.10. Personal Information shall not be uploaded onto an Employee's personal cloud storage accounts or USBs.

Organisational security measures

- 9.2.11. any security incidents concerning Personal Information shall be reported and managed according to the Data Breach Plan.
- 9.2.12. All Personal Information Processed by the Company and other service providers shall be treated as Confidential Information, and be handled with a higher degree of care than ordinary information.
- 9.2.13. Employees shall sign undertakings of confidentiality upon commencing employment.
- 9.2.14. Employees are prohibited from transferring or sending Personal Information to unauthorised Employees, service providers or persons.
- 9.2.15. New Employees must receive induction on and a copy of this Policy.
- 9.2.16. Access to Personal Information should be given to Employees and service providers only on a strictly need to know basis. They may only access information needed for the execution of their required outputs. Under no circumstances will Personal Information be shared outside the scope of required work, for a different purpose, or informally.
- 9.2.17. Employees shall keep all Personal Information secure by taking sensible practical precautions and complying with the data protection rules.
- 9.2.18. Where Personal Information is stored on paper, it shall always be kept in a secure place where an unauthorised person cannot access or see it. This applies to Personal Information stored electronically which has been printed out.
- 9.2.19. Employees should ensure that paper and print outs are not left in places where unauthorised persons can see them, e.g. in unsecured pigeon holes, on a printer or unoccupied desk(s) or unlocked boardroom(s). Printing should be immediately collected from printers.
- 9.2.20. Employees must lock their computer screens and clear their desks when left unattended.
- 9.2.21. In respect of paper files containing Personal Information:
- (a) Employees may not remove files from the Company's administrative premises without prior authorisation from the chairperson;
 - (b) Where permission is granted, Employees must take reasonable measures to secure those files removed and prevent loss, destruction and unauthorised access to such files.

Fax / Email to correct recipients

- 9.2.22. Before sending Personal Information via fax or email, Employees must have previously telephonically confirmed the fax number or email address of the intended recipient.
- 9.2.23. Where practical, frequently used fax numbers and email addresses should be pre-recorded directly on the fax machine and/or emailing system to prevent errors.
- 9.2.24. Employees transmitting highly important Personal Information (i.e. financial information, credit and criminal information, personnel files, etc.) via email must:
- (a) apply password protection to such file and, where feasible, encrypt such file.
 - (b) confirm the identity of intended recipients and inform them of passwords either face to face or by telephone or SMS. Never send out passwords in the same email as the file.

10. DISCLOSURE WITHOUT CONSENT

- 10.1. The Company may be authorised by law, in limited circumstances, to disclose or provide Personal Information to regulatory authorities and other agencies in circumstances where the Consent of person(s) have not been obtained or required.
- 10.2. In the circumstances set out in paragraph 10.1 above, the Company may be obliged to disclose the requested Personal Information, but will first ensure that the request is legitimate and will seek assistance from legal advisers and/or other experts.
- 10.3. Only the Information Officer will be authorised to furnish the requested Personal Information to the enquiring party.

11. DATA BREACHES

- 11.1. Any Employee, supplier or service provider shall immediately notify the Information Officer of any data breach or compromise of Personal or Confidential Information concerning the Company, as soon as they become aware of or ought reasonably to have become aware of such breach, in a manner prescribed by the Breach Notification Form attached to the Company's Data Breach Plan.

12. DIRECT MARKETING

- 12.1. The Company shall not allow Direct Marketing by any of its Employees or service providers using the Personal Information maintained by or on behalf of the Company, except in the limited circumstances where recipients have expressly opted-in (Consented) to receiving such Direct Marketing communications. This includes communications over WhatsApp groups, SMS, email, and other digital platforms whether maintained by the Company or a third party.

13. **EMPLOYEES' CODE OF CONDUCT**

- 13.1. This Policy sets out workplace rules governing the Company's Employees in the course of their work and services to the Company. It shall form part of and is hereby incorporated into the Company's Disciplinary Code and Procedure.
- 13.2. A breach of any rule in relation to the protection of Personal Information set out in this Policy may form the basis of disciplinary action and, in appropriate circumstances, may lead to the dismissal of an Employee.
- 13.3. The imposition of any disciplinary sanction or dismissal shall not preclude the Company from instituting civil proceedings against an Employee who acted in breach of this Policy, negligently or otherwise, and where such breach has resulted in liability, loss, reputational damage and/or other damages to the Company.
- 13.4. Every Employee must familiarise him/herself with the contents of this Policy, and must remain up to date as and when it is notified of any changes to this Policy in writing (including email correspondence).

14. **RESPONSIBLE PARTY FOR PERSONAL AND OTHER CONFIDENTIAL DATA BREACHES**

- 14.1. The Information Officer is responsible for managing Personal Information and other Confidential Information security breaches or other service providers where appropriate.

ANNEXURE A

STATUTORY RETENTION PERIODS

Legislation	Document	Retention Period
Companies Act 71 of 2008	Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act; Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities; Copies of reports presented at the annual general meeting of the company;	7 years

	<p>Copies of annual financial statements required by the Act;</p> <p>Copies of accounting records as required by the Act;</p> <p>Record of directors and past directors, after the director has retired from the company;</p> <p>Written communication to holders of securities and Minutes and resolutions of directors' meetings, audit committee and directors' committees.</p>	
	<p>Registration certificate;</p> <p>Memorandum of Incorporation and alterations and amendments;</p> <p>Rules;</p> <p>Securities register and uncertified securities register;</p> <p>Register of company secretary and auditors and Regulated Companies (companies to which chapter 5, part B, C and Takeover Regulations apply);</p> <p>Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.</p>	Indefinitely
Consumer Protection Act of 2008	<p>Full names, physical address, postal address and contact details;</p> <p>ID number and registration number;</p> <p>Contact details of public officer in case of a juristic person;</p> <p>Service rendered;</p> <p>Cost to be recovered from the consumer;</p> <p>Frequency of accounting to the consumer;</p> <p>Amounts, sums, values, charges, fees, remuneration specified in monetary terms;</p> <p>Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions</p>	3 years
Financial Intelligence Centre Act	<p>Whenever a reportable transaction is concluded with a customer, the institution must keep record of the identity of the customer;</p> <p>If the customer is acting on behalf of another person, the identity of the person on whose behalf the customer is acting and the customer's authority to act on behalf of that other person;</p> <p>If another person is acting on behalf of the customer, the identity of that person and that other person's authority to act on behalf of the customer;</p> <p>The manner in which the identity of the persons referred to above was established;</p> <p>The nature of that business relationship or transaction;</p> <p>In the case of a transaction, the amount involved and the parties to that transaction;</p> <p>All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;</p> <p>The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;</p> <p>Any document or copy of a document obtained by</p>	5 years

	the accountable institution	
Compensation for Occupational Injuries and Diseases Act	Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.	4 years
	Section 20(2) documents : -Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation; -Records of incidents reported at work.	3 years
	Asbestos Regulations, 2001, regulation 16(1): -Records of assessment and air monitoring, and the asbestos inventory; -Medical surveillance records; Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2): -Records of risk assessments and air monitoring; -Medical surveillance records. Lead Regulations, 2001, Regulation 10: -Records of assessments and air monitoring; -Medical surveillance records Noise records - induced Hearing Loss Regulations, 2003, Regulation 11: -All records of assessment and noise monitoring; -All medical surveillance records, including the baseline audiogram of every employee.	40 years
	Hazardous Chemical Substance Regulations, 1995, Regulation 9: -Records of assessments and air monitoring; -Medical surveillance records	30 years
Basic Conditions of Employment Act	Section 29(4): -Written particulars of an employee after termination of employment; Section 31: -Employee's name and occupation; -Time worked by each employee; -Remuneration paid to each employee; -Date of birth of any employee under the age of 18 years	3 years
Employment Equity Act	Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act; Section 21 report which is sent to the Director General	
Labour Relations Act	Records to be retained by the employer are the collective agreements and arbitration awards.	

	An employer must retain prescribed details of any strike, lock-out or protest action involving its employees; Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions	Indefinite
UIF Act	Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed	5 years
Tax Administration Act	Section 29 documents which: -Enable a person to observe the requirements of the Act; -Are specifically required under a Tax Act by the Commissioner by the public notice; -Will enable SARS to be satisfied that the person has observed these requirements	5 years
Income Tax Act	Amount of remuneration paid or due by him to the employee; The amount of employees tax deducted or withheld from the remuneration paid or due; The income tax reference number of that employee; Any further prescribed information; Employer Reconciliation return	
Value-Added Tax Act	Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS; records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques; Documentary proof substantiating the zero rating of supplies; Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.	