

JCE LABOUR LAW t/a GFD GROUP

Corporate Head Office Address: Unit 2, Diaz Convenience
Centre
Mosselbay

CORPORATE MANUAL IN MANAGING JCE LABOUR LAW COMPLIANCE WITH –

- THE PROMOTION OF ACCESS TO INFORMATION ACT, ACT 2 of 2000, (PAIA); and
- THE PROTECTION OF PRIVATE INFORMATION ACT, ACT 4 of 2013 (POPIA)

The Statutory Practices recorded in this Manual are implemented and compliance managed by JCE LABOUR LAW in terms of section 51 of the PAIA and sections 2 and 17 and Regulation 4 (a) of the POPIA and will be in full operation as from 01 July 2021.

Copies of this Manual can be obtained from the Offices of JCE LABOUR LAW as indicated above. Facility Documents created for purposes of the working of the Manual are obtainable from the Information Officer appointed in terms of section 51 of the Promotion of Access to Information Act 2 and sections 1 and 17 of the Protection of Private Information Act at the addresses indicated in this Manual.

01 JULY 2021

CORPORATE STATEMENT

1. **IN ORDER FOR JCE LABOUR LAW TO CONDUCT ITS DAY TO DAY BUSINESS ACTIVITIES, it is necessary that JCE LABOUR LAW will receive and be in possession of, process and present Personal Information** in various forms from and to its Employees, Contractual Suppliers/Service Providers, Clients and/or Customers and/or Individuals and/or Public and Private Institutions and Bodies, which are all Data Subjects in terms of the Acts.
2. JCE LABOUR LAW subscribes to the provisions of the Promotion of Access to Information Act, Act 2 of 2000, which gives effect to the Constitutional Right of Access of a Data Subject to any Information held of a Data Subject by the State and any Information that is held by JCE LABOUR LAW viz a viz its Clients/Data Subjects, and the Right of Access to Information that is held by other Data Subjects in respect of Information that pertains to JCE LABOUR LAW .
 - 2.1 We accept that measures are required for the exercise or protection of any of these Rights, and we accordingly recognize that section 32 (1) (b) of the Constitution provides for the horizontal application of the Right of Access to Information held by another person to everyone when that Information is required for the exercise or protection of any rights; and that the PAIA was enacted to give effect to this right in section 32 of the Constitution. In the light hereof, we will apply the provisions of the PAIA if and when required.
3. Likewise, and in line with the provisions of the Protection of Personal Information Act, Act 04 of 2013, JCE LABOUR LAW will promote the Protection of Personal Information of its Contractual Data Subjects it obtained for lawful Processing and to comply with the conditions introduced by the Act so as to comply with the minimum requirements for the lawful Processing of all Personal Information.
4. We recognise that section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the Right to Privacy and that the Right to Privacy includes a right to Protection against the unlawful collection, retention, dissemination and use of Personal Information.

INDEX

PAGE	CONTENT
2	CORPORATE STATEMENT
4 – 6	DEFINITIONS
PART A	THE PROMOTION OF ACCESS TO INFORMATION ACT (PAIA)
7 – 8	COMPANY AND OTHER RELEVANT INFORMATION
8 – 11	I. PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA (ss 51, 52 of the Act)
11 – 12	II. PROCEDURE FOR A REQUEST FOR ACCESS IN TERMS OF PAIA
12 – 13	III. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA
14	IV. INFORMATION OR RECORDS NOT FOUND
14	V. REMEDIES AVAILABLE TO THE REQUESTER UPON REFUSAL OF A REQUEST FOR ACCESS IN TERMS OF PAIA
14 – 15	VI. DECISION TO GRANT ACCESS TO RECORDS
15	VII. FEES
PART B	THE PROTECTION OF PRIVATE INFORMATION (POPIA)
18 – 19	I. STATUTORY APPOINTMENTS
19	II. CATEGORIES OF DATA SUBJECTS/STAKEHOLDERS
20	III. PERSONAL INFORMATION, DATA CLASSIFICATION AND HANDLING OF PERSONAL INFORMATION
20 – 21	IV. CATEGORIES OF RECIPIENTS AND OPERATORS
21	V. PROCESSING AND PERSONAL INFORMATION PROTECTION POLICY
21 – 22	VI. PERSONAL INFORMATION IMPACT ASSESSMENT
22 – 23	VII. OBJECTION TO PROCESSING OF INFORMATION AND REQUESTS TO DESTROY
23 – 24	VIII. RETENTION AND DESTRUCTION OF INFORMATION RECORDS AND ARCHIVING
24	IX. WITHDRAWAL OF CONSENT
25 – 30	X. GENERAL DESCRIPTION OF OUR PERSONAL INFORMATION SECURITY MEASURES
30 – 31	XI. TRANSBORDER
31	XII. COMPLAINTS
32 – 34	XIII. DIRECT MARKETING

DEFINITIONS FOR PURPOSES OF STATUTORY COMPLIANCE

- 1 **Company** means JCE LABOUR LAW with its particulars as presented above,
- 2 **Conditions for Lawful Processing** means the conditions for the lawful processing
of Personal Information as fully set out in Chapter 3 of POPIA,
- 3 **Constitution** means the Constitution of the Republic of South Africa, 1996,
- 4 **Client** means any natural or juristic person to which JCE LABOUR LAW is a Supplier Vendor
or a Service Provider,
- 5 **Customer** refers to any natural or juristic person that received or receives products and/or services
from JCE LABOUR LAW ,
- 6 **Data Subject "data subject"** means the person to whom personal information relates;
- 7 **Head of the Company** 'head' of, or in relation to, a private body means-
- (a) in the case of a natural person, that natural person or any person duly authorised by that natural person;
 - (b) in the case of a partnership, any partner of the partnership or any person duly authorised by the partnership;
 - (c) in the case of a juristic person-
 - (i) the chief executive officer or equivalent officer of the juristic person or any person duly authorised by that officer; or
 - (ii) the person who is acting as such or any person duly authorised by such acting person;
- 8 **Information Officer** means the JCE LABOUR LAW Chief Executive appointed in terms of the Acts, ((c) in the case of any other public body, means the chief executive officer, or equivalent officer, of that public body or the person who is acting as such),
- 9 **Manual** means this Manual prepared in accordance with section 51 of PAIA and regulation 4 (1) (d) of the POPIA Regulations,
- 10 **PAIA** means the Promotion of Access to Information Act, 2000,
- 11 **Personal Information** means: information about an identifiable individual, including, but not limited to-
- (a) 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 individual;
 - (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

- (c) any identifying number, symbol or other particular assigned to the individual;
- (d) the address, fingerprints or blood type of the individual;
- (e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
- (f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- (g) the views or opinions of another individual about the individual;
- (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and
- (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years,

12 **Personnel** refers to any person who works for, or provides services to or on behalf of JCE LABOUR LAW , and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of JCE LABOUR LAW , which includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff as well as contract workers,

13 **POPIA** means the Protection of Personal Information Act, 2013,

14 **POPIA Regulations** mean the Regulations promulgated in terms of section 112 (2) of POPIA,

15 **Private Body “private body”** means—

- (a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;
- (b) a partnership which carries or has carried on any trade, business or profession; or
- (c) any former or existing juristic person, but excludes a public body;

16 **Processing “processing”** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including —

- (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- (b) dissemination by means of transmission, distribution or making available in any other form; or
- (c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

17 **Responsible Party “responsible party”** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

18 **Record "record"** means any recorded information—

(a) regardless of form or medium, including any of the following:

- (i) writing on any material;
- (ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
- (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
- (iv) book, map, plan, graph or drawing;
- (v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

19 **Requester** 'requester', in relation to—

(a) a public body, means—

- (i) any person (other than a public body contemplated in paragraph (a) or (b) (i) of the definition of 'public body', or an official thereof) making a request for access to a record of that public body; or
- (ii) a person acting on behalf of the person referred to in subparagraph (i);

(b) a private body, means—

- (i) any person, including, but not limited to, a public body or an official thereof, making a request for access to a record of that private body; or
- (ii) a person acting on behalf of the person contemplated in subparagraph (i);

20 **Request for Access** 'request for access', in relation to—

(a) a public body, means a request for access to a record of a public body in terms of section 11; or

(b) a private body, means a request for access to a record of a private body in terms of section 50;21
SAHRC means the South African Human Rights Commission.

PART A PROMOTION OF ACCESS TO INFORMATION ACT COMPLIANCE (PAIA)

1. JCE LABOUR LAW is aware that the objectives of the PAIA are "To give effect to the constitutional right of access to any information held by the State and any information that is held by another person and

that is required for the exercise or protection of any rights; and to provide for matters connected therewith” and regarding the application of the PAIA to JCE LABOUR LAW , we will respect the provisions in the Act and in particular the provision in section 50 of the Act that reads:

“50 Right of access to records of private bodies

(1) A requester must be given access to any record of a private body if-

(a) that record is required for the exercise or protection of any rights;

(b) that person complies with the procedural requirements in this Act relating to a request for access to that record; and

(c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

(2) In addition to the requirements referred to in subsection (1), when a public body, referred to in paragraph (a) or (b) (i) of the definition of 'public body' in section 1, requests access to a record of a private body for the exercise or protection of any rights, other than its rights, it must be acting in the public interest.

(3) A request contemplated in subsection (1) includes a request for access to a record containing personal information about the requester or the person on whose behalf the request is made”

2. JCE LABOUR LAW will in turn expect of Requesters and those acting in terms of the Act, to comply with the provisions of the Act.

COMPANY AND OTHER RELEVANT DETAILS

1. The registration and address details of JCE LABOUR LAW are as follows:

JCE LABOUR LAW t/a GFD Group

Unit 2

Diaz Convenience Centre

Mosselbay

2. Contact details of the Information Officer are as follows:

CHRISTINE LANGEVELD

Diaz Convenience Centre

Mosselbay

headoffice@gfdgroup.co.za

0834356041

3. The SA Human Rights Commission administers the Act and 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.

3.1 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

I. PUBLICATION AND AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA (ss 51, 52 of the Act)

1. JCE LABOUR LAW holds the following statutory and generic Information and Records which in terms of the Act may be available to parties with lawful and legitimate interests in proper request for access.

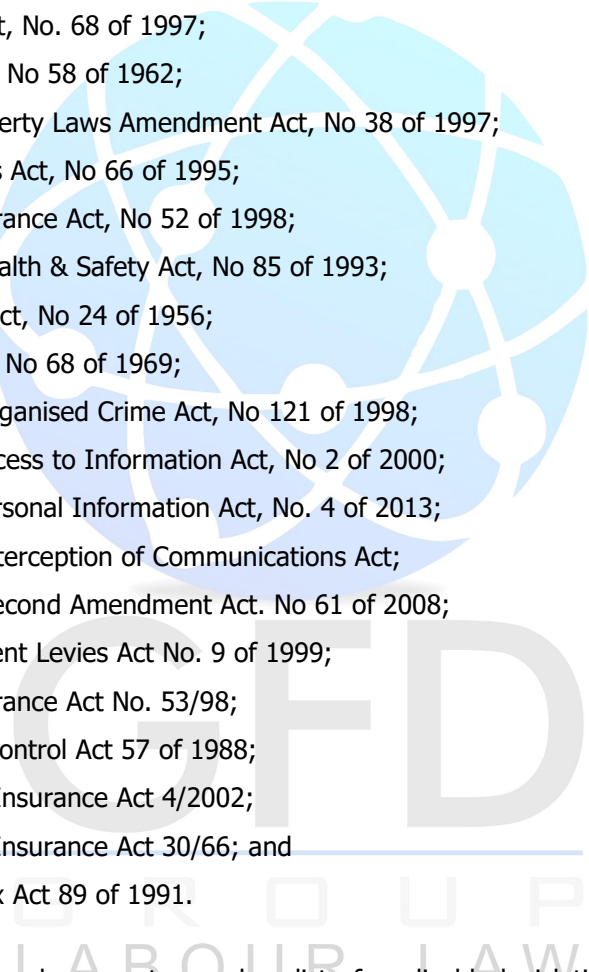
SUBJECT	CATEGORY OF INFORMATION
COMPANIES ACT RECORDS	All Trust Deeds Documents of Incorporation Index of Names of Directors Memorandum of Incorporation Minutes of Meetings Share Certificates

FINANCIAL RECORDS	Accounting Records Annual Financial Reports Annual Financial Statements Asset Registers Bank Statements Banking Details and Bank Accounts Banking Records Debtors/Creditors Statements and Invoices General Ledgers and Subsidiary Ledgers General Reconciliations Invoices Paid Accounts Policies and Procedures Rental Agreements
--------------------------	--

	Tax Returns
INCOME TAX RECORDS	PAYE Records Documents issued to Employees for Income Tax purposes Records of payments made to SARS on behalf of employees <u>All other statutory compliances:</u> VAT issues; Skills Development Levies; Other Levies; UIF; and Workmen's Compensation
PERSONNEL DOCUMENTS RECORDS	Accident Books and Records Address Lists Disciplinary Codes and Records Employee Benefits Arrangements Rules and Records Employment Contracts Employment Equity Plan Forms and Applications, Grievance Procedures Leave Records Medical Aid Records Payroll Reports/Wages Registers Pension Fund Records Health & Safety and Environmental records Salary Records SETA Records Standard Letters and Notices Training Manuals and Training Records Workplace and Union Agreements, Records and other Correspondence.
PROCUREMENT	Standard Terms and Conditions for the Supply of Services and Products Contractor, Client and Supplier Agreements Lists and databases of Suppliers, Products, Services and Distribution Activities.
SALES	Customers' Details Credit Application Information Information and Records provided by a Third Party

2. The following Acts are legislation that may have application in JCE LABOUR LAW . Information in respect hereof are available for inspection unless disclosure is prohibited in terms of Legislation, Regulations, Contractual Agreement or otherwise, the Records that are required to be made available in terms of the Act shall be made available for inspection by Interested Parties in terms of the requirements and conditions of the Act.

1. Auditing Professions Act, No 26 of 2005;
2. Basic Conditions of Employment Act, No 75 of 1997;
3. Broad- Based Black Economic Empowerment Act, No 75 of 1997;
4. Business Act, No 71 of 1991;
5. Companies Act, No 71 of 2008;
6. Compensation for Occupational Injuries & Diseases Act, 130 of 1993;

- 
7. Competition Act, No.71 of 2008;
 8. Constitution of the Republic of South Africa 2008;
 9. Copyright Act, No 98 of 1978;
 10. Customs & Excise Act, 91 of 1964;
 11. Electronic Communications Act, No 36 of 2005;
 12. Electronic Communications and Transactions Act, No 25 of 2002;
 13. Employment Equity Act, No 55 of 1998;
 14. Financial Intelligence Centre Act, No 38 of 2001;
 15. Identification Act, No. 68 of 1997;
 16. Income Tax Act, No 58 of 1962;
 17. Intellectual Property Laws Amendment Act, No 38 of 1997;
 18. Labour Relations Act, No 66 of 1995;
 19. Long Term Insurance Act, No 52 of 1998;
 20. Occupational Health & Safety Act, No 85 of 1993;
 21. Pension Funds Act, No 24 of 1956;
 22. Prescription Act, No 68 of 1969;
 23. Prevention of Organised Crime Act, No 121 of 1998;
 24. Promotion of Access to Information Act, No 2 of 2000;
 25. Protection of Personal Information Act, No. 4 of 2013;
 26. Regulation of Interception of Communications Act;
 27. Revenue laws Second Amendment Act. No 61 of 2008;
 28. Skills Development Levies Act No. 9 of 1999;
 29. Short-term Insurance Act No. 53/98;
 30. Trust Property Control Act 57 of 1988;
 31. Unemployment Insurance Act 4/2002;
 32. Unemployment Insurance Act 30/66; and
 33. Value Added Tax Act 89 of 1991.

- 2.1 We have used our best endeavours to supply a list of applicable legislation; it is possible however that this list may be incomplete. Whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly.
- 2.2 If a Requester believes that a Right of Access to a Record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what Statutory Right the Request is based on, to allow the Information Officer the opportunity of considering the request in light thereof.

3. It is further recorded that the accessibility of documents and records may be subject to the grounds of refusal set out in this PAIA Manual.

II. PROCEDURE FOR A REQUEST FOR ACCESS IN TERMS OF PAIA

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.
2. A Requester must complete the prescribed Request for Access form attached as Annexure A, and submit the completed Request for Access form as well as payment of a request fee or a deposit as arranged to the Information Officer at the postal or physical address, facsimile number or electronic mail address above.
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, should the request be 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.
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.
5. If an individual is unable to complete the prescribed Form because of illiteracy or disability, such a person may make the request orally.
6. JCE LABOUR LAW 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.

7. We will process the request within 30 (thirty) days, unless the Requester has stated special reasons, to the satisfaction of the Information Officer, that circumstances dictate that the above time periods not be complied with.
8. The requester shall be advised whether access is granted or denied in writing. If, in addition, the Requester requires the reasons for the decision in any other manner, the requester will be obliged to state in which manner the particulars are required.
9. All detail required as mentioned above should be provided and failing which, the process will be delayed until the required information is provided. The prescribed time periods will not commence until the requester has furnished all the necessary and required information.

III. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS IN TERMS OF PAIA

1. The following are the Grounds on which JCE LABOUR LAW may, subject to the exceptions contained in Chapter 4 of PAIA, refuse a Request for Access in accordance with Chapter 4 of PAIA:
 - 1.1 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;
 - 1.2 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;
 - 1.3 mandatory protection of confidential information of third parties if it is protected in terms of any agreement;
 - 1.4 mandatory protection of the safety of individuals and the protection of property;
 - 1.5 mandatory protection of Records that would be regarded as privileged in legal proceedings;

- 1.6 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;
- 1.7 research information of JCE LABOUR LAW or a third party, if such disclosure would place the research or the researcher at a serious disadvantage; and
- 1.8 requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

IV. INFORMATION OR RECORDS NOT FOUND

1. Should JCE LABOUR LAW be unable to find the Records that the Requester is looking for, despite reasonable and diligent search(es), 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(s) and accordingly the inability to locate the Document(s)/Record(s).

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

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.
2. In accordance with sections 56 (3) (c) and 78 of PAIA, a Requester may after notification of the Decision apply to a Court for appropriate relief. For purposes of the Act, the Courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status and a Magistrate's Court designated by the Minister of Justice and Constitutional Development and which is presided over by a designated Magistrate.

VI. DECISION TO GRANT ACCESS TO RECORDS

1. The Company will decide whether to grant or decline the Request for Access within 30 (thirty) days of receipt of the Request for Access and must give notice to the Requester with reasons (if required) to that effect.
2. The period referred to above may be extended for a further period of not more than 30 (thirty) 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 (thirty) day period.
3. The Company will notify the Requester in writing should an extension of time as contemplated above be required.
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.

VII. FEES

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.

2. 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.
3. Re Prescribed Fees (Section 51 (1) (f)), we advise that the Act provides for two types of fees, namely:
 - 3.1 A request fee, which is a form of administration fee to be paid by all requesters except personal requesters, before the request is considered and is not refundable; and
 - 3.2 An access fee, which is paid by all requesters in the event that a request for access is granted. This fee is inclusive of costs involved by the private body in obtaining and preparing a record for delivery to the requester.

PART B. PROTECTION OF PERSONAL INFORMATION ACT COMPLIANCE (POPIA)

1. This Manual is issued bearing in mind that the purpose of the POPIA is to give effect to our Data Subject Clients and Suppliers' Constitutional right to Privacy, by safeguarding their Personal Information when processed by our Information Officer and/or Responsible Party, subject to justifiable limitations that are aimed at balancing the right to their privacy against other rights.
- 1.1 This is to take place while understanding the need for the free flow of information needed for our and our Business Partners' legitimate interests.
2. These Practices are also implemented realising that in terms of sections 60 to 68 of the Act, the Information Regulator will develop and in appropriate circumstances promulgate Codes of Conduct for purposes of clarifying how the conditions and any exemptions which may have been granted are to be applied, or are to be complied with.

3. We recognise that our Employees, Customers, Clients, Suppliers and Business Partners being Data Subjects have the right to have his, her or its Personal Information processed in accordance with the Conditions for the Lawful Processing of Personal Information as contained in Chapter 3 of the Act, including the right — (see section 5 of the Act)

3.1 "(a) to be notified that —

- 1 (i) personal information about him, her or it is being collected as provided for in terms of section 18; or
- (ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;
- (b) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;
- (c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;
- (d) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)(a);
- (e) to object to the processing of his, her or its personal information—
 - (i) at any time for purposes of direct marketing in terms of section 11(3)(b); or
 - (ii) in terms of section 69(3)(c);
- (f) not to have his, her or its personal information processed for purposes of Direct Marketing by means of unsolicited electronic communications except as referred to in section 69(1);
- (g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;
- (h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and
- (i) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

4. Our Information Officer will in a spirit of Openness consider the publicising of the purpose for any Private Information processed by us and will in an ongoing manner maintain the Documentation of all Processing Operations under his responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act. We may contract Suppliers to assist us in upkeep of our Policies and Procedures.

4.1 The actions herein will comply with regulation 4 issued by the Regulator that reads:

"Responsibilities of Information Officers

4. (1) An information officer must, in addition to the responsibilities referred to in section 55 (1) of the Act, ensure that-

- (a) a compliance framework is developed, implemented, monitored and maintained
 - (b) a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information;
 - (c) a manual is developed, monitored, maintained and made available as prescribed in sections 14 and 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);
 - (d) internal measures are developed together with adequate systems to process requests for information or access thereto; and
 - (e) internal awareness sessions are conducted regarding the provisions of the Act, regulations made in terms of the Act, codes of conduct, or information obtained from the Regulator.
- (2) The information officer shall upon request by any person, provide copies of the manual to that person upon the payment of a fee to be determined by the Regulator from time to time"

5. This Manual also seeks to identify and set standards of our Security Safeguards and implement Security Measures on Integrity and Confidentiality of Personal Information.

5.1 These measures maintained by our Information Officer/Responsible Party secure the integrity and confidentiality of Personal Information in our possession or under our control by taking appropriate, reasonable technical and organisational measures to prevent—

- (a) loss of, damage to or unauthorised destruction of personal information; and
- (b) unlawful access to or processing of personal information.

Our Responsible Party will also take reasonable measures to —

- (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- (b) establish and maintain appropriate safeguards against the risks identified;
- (c) regularly verify that the safeguards are effectively implemented; and
- (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

6. Therefore this Manual is promulgated and Facility Documents provided to implement the Program and to assure statutory compliance to the Act. See our Letter to our Staff, Contractors and Vendors in our Training and Awareness Folder that reveal our commitment to compliance with POPI Legislation in this regard.

I. STATUTORY APPOINTMENTS

1. Statutory Appointments for purposes of the POPIA is done and are the same as for the purposes of the PAIA indicated above. (Copies of the Certificates of Appointment are stored in our PAIA and POPIA Compliance Folders)
2. We are aware that the Information Officers are required, in terms of Section 55 (2) of POPIA, to take up their duties only after being registered with the Regulator and that the Information Officers referred to in section 55 (1) of POPIA are the same Information Officer referred to in sections 1 or 14 and 51 of PAIA.
3. The Information Officers of public or private bodies perform their duties and responsibilities in terms of both PAIA and POPIA. For a copy of Offences and other issues pertaining our Information Officer see our Compliance Folders.

II. CATEGORIES OF DATA SUBJECTS/STAKEHOLDERS

1. The Caption to the POPIA reads that: To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.
2. The Definitions in chapter 1 of the Act defines a Data Subject as follows: “data subject’ means the person to whom personal information relates”, and it is accordingly clear that the duties owed by JCE LABOUR LAW are against persons who’s information the Boerdery processes.

2.1 Person again is defined as “‘person’ means a natural person or a juristic person”;

3. Our Data Subjects accordingly are:

- Our employees;
- Our clients/customers;
- Our suppliers/vendors and service providers; and
- Persons with whom JCE LABOUR LAW is in Voluntary and Business Associations.

3.1 Statutory Compliance will be in respect of Data Subjects mentioned in par 3 above.

PERSONAL INFORMATION AGREEMENTS WITH OUR EMPLOYEES

4. For copies of our Agreements with Staff in this regard see copies of the Agreements in our Compliance Folders.

III. PERSONAL INFORMATION, DATA CLASSIFICATION AND PRIVACY SECURITY AWARENESS

1. “**personal information**’ means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to —
 - (a) 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;
 - (b) information relating to the education or the medical, financial, criminal or employment history of the person;
 - (c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
 - (d) the biometric information of the person;
 - (e) the personal opinions, views or preferences of the person;
 - (f) 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;
 - (g) the views or opinions of another individual about the person; and
 - (h) 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”

2. Our Information Classification and Information Handling Policy is included in our Compliance Folders, and shall be complied with and developed further in our operations.
3. Our Staff Members are constantly required to develop an awareness and culture for privacy of Information, quality of Information and security of Information - as is required in the Act.
4. See our JCE LABOUR LAW Training Notes on the Classification and Handling of Personal Data Subjects' Information included in the JCE LABOUR LAW Compliance Folders.

IV. CATEGORIES OF RECIPIENTS AND OPERATORS

1. Data Subject/Personal Information is received by our Information Officer, Responsible Person and our Employees for our lawful Processing and use.
2. The definitions in the Act indicate the difference between a Responsible Person and an Operator.
 - 2.1 It is our understanding that if a person exercises Overall Control of the purpose and means of the processing of personal information i.e. that Person decides which Personal Information is to be processed and why, - that Person is a Responsible Person.
 - 2.2 If a Person does not have any purpose of his own for Processing the data and that Person only acts on a Client's instructions, that person is an Operator in our business.

V. PROCESSING AND PERSONAL INFORMATION PROTECTION POLICY

1. "Processing" means – any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including —
 - (a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - (b) dissemination by means of transmission, distribution or making available in any other form; or
 - (c) merging, linking, as well as restriction, degradation, erasure or destruction of Information"

INFORMATION PROTECTION

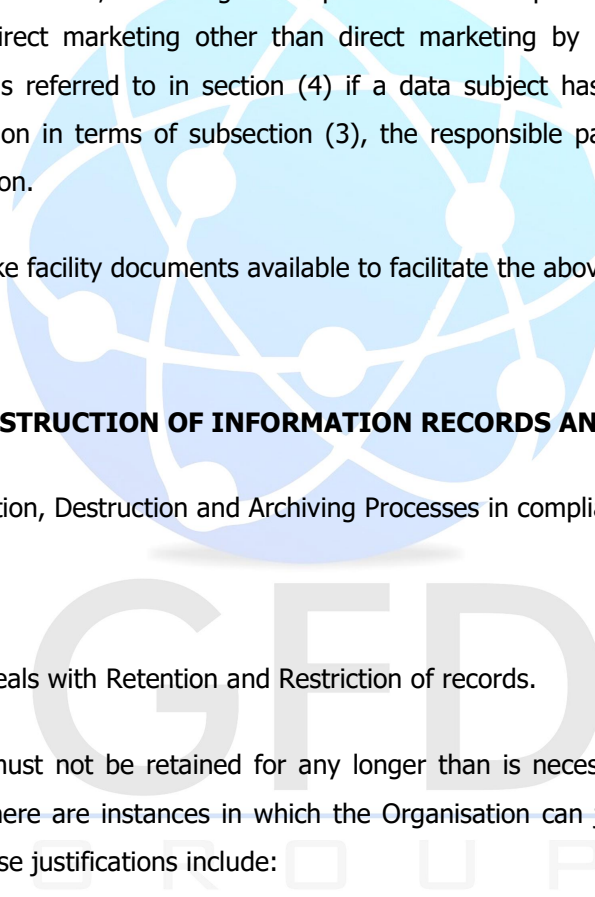
2. Our Personal Information Protection Policy (See Compliance Folder for a copy) is a document that contains particulars how our organisation protects Personal information and how we continually develop it in terms of the Act. It is a set of principles, rules and guidelines that informs how we ensure ongoing compliance with data protection laws.

VI. PERSONAL INFORMATION IMPACT ASSESSMENT (PIIA)

1. A personal information impact assessment (PIIA) is an instrument for assessing the potential impacts that a Process, Information System, Programme, Software Module, Device or other Initiative may have on the Information. Our PIIA is a process to guarantee Privacy by design and will be developed and refined continually.
2. Regulation 4 (1) stipulates that an Information Officer must ensure that a personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
3. We created a Personal Information Impact Assessment and a copy can be obtained from our Compliance Folders. The Assessments will be refined on a continual basis.

VII. CONSENT, JUSTIFICATION AND OBJECTION TO PROCESSING OF INFORMATION AND REQUESTS TO DESTROY

1. We are aware that section 11 contained in chapter 3 of the Act determines:
"11. (1) Personal information may only be processed if —
 - (a) the data subject or a competent person, where the data subject is a child, consents to the processing;
 - (b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
 - (c) processing complies with an obligation imposed by law on the responsible party;
 - (d) processing protects a legitimate interest of the data subject;
 - (e) processing is necessary for the proper performance of a public law duty by a public body; or
 - (f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

- 
- (2) (a) The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1) (a).
- (b) The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1) (a), at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1) (b) to (f) will not be affected.
- (3) A data subject may object, at any time, to the processing of personal information—
- (a) in terms of subsection (1) (d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
- (b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section (4) if a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information.
2. We will create and make facility documents available to facilitate the above statutory processes.

VIII. RETENTION AND DESTRUCTION OF INFORMATION RECORDS AND ARCHIVING

1. We manage our Retention, Destruction and Archiving Processes in compliance with the POPIA.

RETENTION PERIODS

2. Section 14 (1) to (3) deals with Retention and Restriction of records.
3. Personal information must not be retained for any longer than is necessary to achieve the purpose of collection. However, there are instances in which the Organisation can justify retaining the information for longer periods. These justifications include:
- (a) Retaining the information because it is required or authorised by law;
- (b) Retaining the information because the Organisation requires the information for lawful purposes related to its functions or activities;
- (c) Retaining the information as it is required by a contract between the parties; or
- (d) Retaining the information because a data subject, or a competent person in the case of a child, consents to the retention.

RESTRICTION OF PROCESSING Section 14 (4)

4. Restriction of Processing Personal Information must take place in the following circumstances:
 - (a) If the data subject is contesting the accuracy of the information, the processing must be restricted while the Organisation investigates the accuracy of the information.
 - (b) If the Organisation no longer needs the personal information to achieve the purpose for which it was collected but is retaining it as proof or for historical purposes, the Organisation must not process the personal information for any reason.
 - (c) the Organisation was processing the personal information without a lawful justification, the data subject can request that the information must be restricted instead of being destroyed.
5. Restriction means that an Organisation may only store it or use it for proof. However, the restriction will be lifted if:
 - (a) processing the information is in the public interest;
 - (b) the information is being processed for the protection of another data subject; or
 - (c) the Organisation has the data subject's consent to resume processing.
6. Our Record Retention and Disposal Policy is included in our Compliance Folder.
7. Section 8 (Retention and Restriction of Records) stipulates that the Responsible Party must ensure that the conditions set out in the POPIA, and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the Processing itself. We will accordingly develop and operate an archiving system. Likewise, will we keep a disposal register.

IX. WITHDRAWAL OF CONSENT

1. We acknowledge a Data Subject can give consent to the Processing of his Personal Information but likewise we acknowledge that such consent can be withdrawn.
2. We are aware that the normal legal requirements for a lawful consent are required for the withdrawal of consent once given.

X. GENERAL DESCRIPTION OF OUR PERSONAL INFORMATION SECURITY MEASURES

SECURITY RISK ASSESSMENT

1. Section 19 (2) stipulates that in order to give effect to section 19 (1), the Responsible party must take reasonable measures to -
 - (a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
 - (b) establish and maintain appropriate safeguards against the risks identified;
 - (c) regularly verify that the safeguards are effectively implemented; and
 - (d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
2. Section 109 (3) (g) then provides that when determining an appropriate fine the Regulator must consider certain factors, including any failure to carry out a risk assessment or a failure to operate good policies, procedures and Organisations to protect Personal information.
3. A Risk Assessment is the process of identifying, analysing and evaluating threats and vulnerabilities. In an information security context, risk assessments are crucial for working out the ways cyber criminals and employees might compromise Personal information.
4. Our Security Risk Assessment Policy is contained in the Compliance Folders and will be complied with.
5. See our letter to Staff re our Security Culture survey, and our Letter to Leadership re the issue in our Compliance Folders.
6. Further Risk Assessment i.r.o. Security Measures and Storage re the Integrity and Confidentiality of our Personal are done i.t.o. section 19 of the Act. Same may be drafted into Policy if needed.
7. Section 19 of the Act reads:

“19. (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

 - (a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations”

7.1 This Training Notes will be issued and shall be adhered to by JCE LABOUR LAW Staff. We do this in view of Section 109 (3) (g) that provides that when determining an appropriate fine the Regulator must consider certain factors, including any failure to carry out a risk assessment or a failure to operate good policies, procedures and Organisations to protect personal information.

8. We view Training Notes as our Risk Assessment which is the Process of Identifying, analysing and evaluating Threats and Vulnerabilities. Training Notes may lead to creation of further Policies.

INVENTORY OF OUR PERSONAL INFORMATION RECORD KEEPING MACHINERY AND TOOLS

- STAFF

9. We realise that the most vulnerable component of any Information System is the people who work with it.

10. We employ the following groups of employees who are responsible for Processing Purposes and will be trained in POPIA compliance.

1	Management
2	Workers
3	Private Contractors
4	Our Professional Service Providers (Accountants/attorneys/financial and other advisors)
5	Contractors and Business Associates

6	Part-time/temporary staff, agency staff
7	Visitors, Guests, Salespeople, Reps from time to time

- DEVICES

11. In our actions to keep proper and reliable Personal Information and Records accounts we need to determine what Controls are in place and available and used by us.

11.1 We view it as necessary to be able to definitively declare the number of individual Personal Information Records in our control and where/on which devices the Records and Information are contained/located.

12. The following are the assets that we have and utilize in our operations. We will in our development of our Controls Instruments in POPIA view and address more detailed issues and matters of security, and draft same into our Notes and Policies.

1	Desktop computers and drives
2	On-site server
3	Cloud capacities
4	Laptops
5	Tablets
6	Smartphones
7	External/portable hard drives
8	CDs/DVDs/VHS/Other Media
9	USB "flash" drives
10	Tapes or other removable media
11	Printers, scanners, fax machines with internal memory (data cache)

13. Other Security Measures and Safeguards (Physical and Administrative)

1	Access control to enter the premises
2	The premises are locked during and after business hours
3	Intrusion alarms are used after business hours
4	Unescorted visitors are prevented from entering secure parts of the premises
5	Removable media is physically secured when not in use
6	Smoke/fire alarms are functional
7	Electronic components are protected from power surges/spikes
8	Critical components are powered via uninterruptable power supplies
13	Devices are protected from theft
14	Name badges, access cards etc. are inventoried and controlled
15	There is video surveillance
16	There is off-site backup
17	Documents to be destroyed are disposed of securely
18	Devices storing confidential information are disposed of securely
19	There is a designated "Information Officer"
20	Periodic privacy and security audits will be performed in POPI compliance
21	There is a clear procedure for managing a suspected or actual privacy breach
22	We address retention/archiving/destruction/disposal of physical records, images, media, devices, computers, photocopiers, etc.
23	We address retention/archiving/destruction of personal information
24	There is a process with accountability for policy development and assessment
25	POPI Operator Agreements are in place with all vendors and contractors who create, receive, maintain (store) or transmit personal information
26	Organisational data sharing agreements are in place where appropriate
27	We address the use of portable devices (e.g., laptops, tablets, smartphones, flash drives, CDs/DVDs etc.)

28	We address password management (e.g. complexity, strength provisioning, de-provisioning, expiration, sharing etc.)
29	Users are forced to change passwords periodically
30	Records are kept of physical access to the facility by staff (especially after hours) and visitors ("COVID-19 Visitor Log")
31	Records are kept of maintenance to critical physical systems
32	There is a process for documenting training
33	There is a process for evaluating correct use and adequate skills among users

14. We realize the importance of Technical Safeguards and accordingly and in line with POPIA requirements make sure that:

1	Appropriate firewalls are in place and being kept up to date
2	Anti-virus, anti-Hashing, anti-spyware/adware protections are in use; updates are timely installed
3	Data is backed up; backup files are encrypted
4	Data backup (on-site and off-site) and restore functions are regularly tested
5	Routers and Wi-Fi access points are secured; Wi-Fi is encrypted; default administrator ID and password have been changed
6	Devices are password protected
7	E-mail system for internal users is encrypted and protected
8	Access to confidential information is controlled using unique IDs
9	Access to confidential information is restricted according to user roles
10	Users are automatically logged-off after a period of inactivity

15. JCE LABOUR LAW is constantly developing strategies to deal with Natural and Man-Made disasters. Under Natural Disaster we deal with hail, wind, blizzard, ice storm, flood, storm surge, fire, lightning, pandemic; and under man made we make provision for infrastructure and criminal activities.

16. In our ongoing development of measures to comply with vulnerabilities, technical and administrative threats, risks and other impacts on our Business and Personal Information practices, we will in view of statutory requirements develop best practices to address possible environmental threats, physical threats like theft, vandalism, inclement weather etc.

XI. TRANSBORDER

1. We are aware of the provisions of section 72 of the Act and accordingly our Responsible Party will abide in with the following:

"72. (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that —

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

(ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

(b) the data subject consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(e) the transfer is for the benefit of the data subject, and —

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

(2) For the purpose of this section—

(a) "binding corporate rules" means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

(b) "group of undertakings" means a controlling undertaking and its controlled undertakings.

XII. COMPLAINTS / SECURITY BREACH NOTIFICATION

1. The POPIA requires that a responsible party must notify the Information Regulator and data subjects in case of unauthorised access to personal information.

The notification must meet the following requirements:

- The notification must take place as soon as reasonably possible after the security incident is discovered.
- The notification must not compromise the ability of law enforcement (or another public body) to investigate the breach or the ability of the responsible party to determine the scope of the incident and to restore the integrity of the responsible party's information system. In other words, there may be circumstances when it is necessary to keep the incident confidential while it is being investigated.
- The notification must be in writing and must be communicated through at least one of the following communication channels: by post, by email, announced in a prominent position on the responsible party's website, published in news media or any other channel determined by the Information Regulator.
- The notification must contain enough information to allow data subjects to take steps to protect themselves against the consequences of the security breach. The notice must include a description of the possible consequences of the breach, measures the responsible party will take to address it, recommendations for the measures the data subject can take to minimise the effect of the breach, and the identity of the unauthorised person(s) who may have accessed or acquired the information.

XIII. DIRECT MARKETING

1. We are aware that most complaints received by Information Regulator relates to unsolicited "direct marketing".

2. Although we do not foresee engaging in direct unsolicited marketing, it is prudent that our Staff take note of some aspects of direct marketing should the issue appear in our Business Dealings.
3. The concept of Direct Marketing in the POPIA contains the following elements:
 - the communication must be directed at an identified or identifiable data subject or group of data subjects;
 - the communication must be in the form of an 'electronic communication'; and
 - the communication must have the direct or indirect purpose of promoting a business or goods or services or to request donations.
4. For a communication to qualify as direct marketing it must be directed at an identified or identifiable data subject or group of data subjects. When a Responsible Party is in possession of a data subject's contact details, marketing transmitted to those contact details will be considered 'direct marketing' as the marketer is targeting that data subject.
5. Direct marketing can also be transmitted via social media platforms to 'custom audiences'. When targeting a custom audience, a marketer typically provides the social media platform with contact details in its database which the social media platform then matches with users who are then specifically targeted.
6. The definition of 'direct marketing' in section 1 refers to marketing done in person, by mail, or by "electronic communication". While the other provisions of the POPIA will apply to all forms of direct marketing, section 69 that regulates when consent is required, only applies to 'electronic communications'.
7. The POPIA defines "electronic communication" as messages 'sent over an electronic communications network which is stored in the network or the recipient's terminal equipment until it is collected by the recipient'
- 7.1 Electronic communication includes:
 - email;
 - SMS;
 - Fax;
 - Automatic calling machines;
 - Direct messaging via social media; and

- Advertising through social media platforms or display banners when a custom audience is targeted.

8. The following types of communication will not be subject to section 69 of the POPIA:

- approaching a data subject in person;
- telemarketing (unless it is made by automatic calling machines or the telemarketer leaves a voice message); and
- mail (post).

9. Even though section 69 does not apply to these forms of communication, the rest of the POPIA is still applicable. For instance, the direct marketing activity will still have to be justified in terms of section 1 and the POPIA will determine whether the personal information used in the direct marketing was collected from a lawful source.

10. Direct marketing by approaching a data subject in person, by telephone, or mail is also regulated by the Consumer Protection Act (the CPA). Section 11 of the CPA provides that direct marketing may be sent unless the consumer has pre-emptively blocked direct marketing, or unsubscribes.

11. The POPIA states that, in order to send direct marketing, an institution must obtain the data subject's consent. To decide whether consent is required, it is important to distinguish between instances where the marketers approached the recipient and instances where the recipient solicited the marketing from the marketer.

An opt-in consent is not required if:

- the recipient contacts the marketer to enquire about or purchase goods or services;
- the recipient is told that the recipient's personal information would be used to send marketing communications;
- the marketer only sends marketing communication for its own goods or services, and those goods or services are similar to the ones the recipient contacted the marketer about or purchased;
- the recipient is given an opportunity to unsubscribe at the time the personal information was collected (i.e. the recipient was given an opportunity to opt out); and
- the recipient can unsubscribe every time the recipient receives marketing communications.

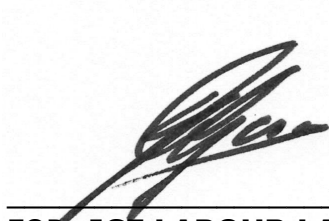
An opt-in is also not required if institutions can ensure that they:

- can prove when and where they obtained the information and whether it was in the context of the sale of a product or a service;
 - only sent direct marketing for the same or similar products or services;
 - can prove that they gave the data subject the opportunity to unsubscribe at collection; and
 - always gave the data subject an opportunity to unsubscribe in subsequent communications.
12. An institution cannot send unsolicited direct marketing without the data subject's consent. The POPIA states that if data subjects have previously declined to give consent to receive direct marketing, they may not be approached again.
13. The consent obtained from the data subject must be valid in order for the direct marketing to be lawful.

These Statutory Practices are implemented and compliance managed by JCE LABOUR LAW in terms of section 51 of the PAIA and sections 2 and 17 and Regulation 4 (a) of the POPIA and will be in full operation as from 01 July 2021.

Our Manual is created in a broader statutory Framework which is implemented and developed on a continual basis. It will be monitored and maintained in line with paragraph 4 of Regulation No. R. 1383 of 14 December 2018.

Copies of this Policy can be obtained from the Offices of JCE LABOUR LAW as indicated above. Facility Documents created for purposes of the working of the Manual are obtainable from the Information Officer appointed in terms of section 51 of the Promotion of Access to Information Act 2 and sections 1 and 17 of the Protection of Private Information Act at the addresses indicated in this Manual.



FOR: JCE LABOUR LAW t/a GFD Group