GERT NEL INCORPORATED

REGISTRATION NUMBER: 2006/008065/21

MANUAL IN TERMS OF SECTION 51 OF THE PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000, AS AMENDED

Date of compilation : 25 October 2023

Date of revision : 09 September 2024

1. INTRODUCTION

1.1 The Promotion of Access to Information Act 2 of 2000 (hereinafter 'PAIA') was enacted for the purpose of giving effect to the constitutional right of access to information and to promote the transparent, accountable and effective governance of all public and private bodies.

1.2 Gert Nel Incorporated is a South African law firm specialising in personal injury law and is duly incorporated as such in terms of the company laws of the Republic of South Africa (hereinafter 'the Republic'). Gert Nel Incorporated (hereinafter 'GNI') falls within the ambit of a 'private body' as defined in section 1 of PAIA and is therefore required to comply with its requirements.

1.3 Section 51 of PAIA requires the head of a private body to make available a manual, the purposes of which are expounded upon in part 2 below.

2. PURPOSES OF MANUAL

The PAIA manual is useful for the public to –

2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;

2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;

2.3 know the description of the records of the body which are available in accordance with any other legislation;

2.4 access all relevant contact details of the Information Officer (hereinafter 'IO') and Deputy Information Officer (hereinafter 'DIO') who will assist the public with the records they intend to access;

2.5 know the description of the guide on how to use PAIA, as updated by the Information Regulator (hereinafter 'the Regulator') and how to obtain access to it;

2.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;

2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;

2.8 know the recipients or categories of recipients to whom the personal information may be supplied;

2.9 know if the body has planned to transfer or process personal information outside the Republic and the recipients or categories or recipients to whom the personal information may be supplied; and

2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. INFORMATION REQUIRED BY SECTION 51(1)(a) OF PAIA

3.1	Information Officer:	Gert Elias Paulus Nel
	Position:	Director
	Tel:	+27 (0) 12 333 8990 #104
	Email:	gert@gertnelattorneys.co.za
	Fax:	+27 (0) 12 333 8991

3.2 Deputy Information Officer(s): None

3.3 Postal address of the head of the body

P.O. BOX 11614, Queenswood, Pretoria, 0186

3.4 Street address of the head of the body

345 Clark Street, Waterkloof, Pretoria, 0181

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1 The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available a revised guide on how to use PAIA (hereinafter 'the Guide'), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2 Section 51(1)(b) of the PAIA requires a private body to include a description of the Guide in its manual, along with guidance on how to obtain access to it, as is provided in this section

4.3 The Guide is available in each of the official languages and in braille.

4.4 The Guide contains the description of –

4.4.1 the objects of PAIA and POPIA;

4.4.2 the postal and street addresses, phone and fax numbers and, if available, the electronic mail addresses of –

4.4.2.1 the IO of every public body; and

4.4.2.2 every DIO of every public and private body designated in terms of section 17(1) of PAIA[1] and section 56 of POPIA[2];

4.4.3 the manner and form of a request for –

4.4.3.1 access to a record of a public body contemplated in section 11[3]; and

4.4.3.2 access to a record of a private body contemplated in section 50[4];

---

1 **Section 17(1) of PAIA –**

For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.

2 **Section 56(a) of POPIA –**

Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.

3 **Section 11(1) of PAIA –**

A requester must be given access to a record of a public body if that requester complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

4 **Section 50(1) of PAIA –**

A requester must be given access to any record of a private body if

4.4.4 the assistance available from the IO of a public body in terms of PAIA and POPIA;

4.4.5 the assistance available from the Regulator in terms of PAIA and POPIA;

4.4.6 all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging –

4.4.6.1 an internal appeal;

4.4.6.2 a complaint to the Regulator; and

4.4.6.3 an application with a court against a decision by the IO of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;

4.4.7 the provisions of sections 14[5] and 51[6] requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

---

a) That record is required for the exercise or protection of any rights;
b) that person complies with the procedural requirements in PAIA 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.*

5 **Section 14(1) of PAIA –**

The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.

6 **Section 51(1) of PAIA –**

The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.

4.4.8 the provisions of sections 15[7] and 52[8] providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.4.9 the notices issued in terms of sections 22[9] and 54[10] regarding fees to be paid in relation to requests for access; and

4.4.10 the regulations made in terms of section 92[11].

4.5 Members of the public can inspect or make copies of the Guide from the officers of the public and private bodies, including the office of the Regulator, during normal working hours.

4.6 The Guide can also be obtained –

---

7 **Section 15(1) of PAIA:**

The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access

8 **Section 52(1) of PAIA:**

The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access

9 **Section 22(1) of PAIA:**

The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

10 **Section 54(1) of PAIA:**

The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

11 **Section 92(1) of PAIA:**

The Minister may, by notice in the Gazette, make regulations regarding –

(a) any matter which is required or permitted by this Act to be prescribed;
(b) any matter relating to the fees contemplated in sections 22 and 54;
(c) any notice required by this Act;
(d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and
(e) *any administrative or procedural matter necessary to give effect to the provisions of this Act.*

4.6.1 upon request to the IO;

4.6.2 from the website of the Regulator (https://www.justice.gov.za/informed).

4.7 A copy of the Guide is also available in the following two official languages, for public inspection, during normal office hours –

4.7.1 English, Afrikaans

5. CATEGORIES OF RECORDS OF GNI WHICH ARE AVAILABLE WITHOUT A PERSON HAVING TO REQUEST ACCESS

To date, no notice(s) in terms of section 52(2) of PAIA have been published on categories of records that are automatically available without a person having to request access in terms of PAIA.

6. RECORDS OF GNI WHICH ARE AVAILABLE IN ACCORDANCE WITH LEGISLATION

Records are kept in accordance with the legislation applicable to GNI, including but not limited to the following:

Administration of Estates Act 66 of 1965
Basic Conditions of Employment Act 75 of 1997
Broad Based Economic Empowerment Act 53 of 2003
Companies Act 61 of 1973
Companies Act 71 of 2008
Compensation for Occupational Injuries and Diseases Act 120 of 1993
Constitution of the Republic of South Africa 108 of 1996
Consumer Protection Act 68 of 2008

Contingency Fees Act 66 of 1997
Electronic Communications and Transactions Act 36 of 2005
Employment Equity Act 55 of 1998
Financial Intelligence Centre Act 38 of 2001
Income Tax Act 58 of 1962
Labour Relations Act 66 of 1995
Legal Practice Act 28 of 2014
National Credit Act 34 of 2005
Occupational Health and Safety Act 85 of 1993
Pension Funds Act 24 of 1956
Promotion of Access to Information Act 2 of 2000
Protection of Personal Information Act 4 of 2013
Securities Transfer Tax Act, 2007
Securities Transfer Tax Administration Act, 2007
Skills Development Act 97 of 1988
Skills Development Levies Act 9 of 1999
Tax Administration Act, 2011
Unemployment Contribution Act 4 of 2002
Unemployment Insurance Act 30 of 1996
Value Added Tax Act 89 of 1991

7. DESCRIPTION OF THE SUBJECTS ON WHICH GNI HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY GNI

Subjects on which GNI holds records	**Categories of records**
Accounting records and financial documents	Accounting records Annual financial statements Asset register Auditors' reports Bank statements Cheques pad

	Debit notes Cash records Credit notes Cheque account Current account Electronic banking records Financial reporting General ledger Invoices Subsidiary ledgers Tax returns and assessments VAT returns
Contracts	Agreements with shareholders, officers, and directors Contracts with third parties
Clients	All pleadings, documents, and notices relevant to a client's file, including, but not limited to, agreements, consultation notes, correspondence, documentary, orders, proof, memoranda, notices, powers of attorney, and statements of account.
Statutory company records	Certificate of incorporation Memorandum of incorporation Minutes of board meetings, firmwide attorneys' meetings and other meetings Securities register Resolutions Shareholders agreements Records regarding property
Intellectual property	Designs, trademarks, trade names, and protected names

Environmental Health and Safety	Emergency response plans
Human resources	Employment contracts Educational history Disciplinary codes Disciplinary records IRP5 and IT3 certificates Leave records Letters of employment Medical history of employees Performance management records Personality and psychometric test records Policies and procedures Records of incidents and corrective action Salary records Tax records Training and development records UIE, PAYE, and SDL returns Workplace Skills and Development Plan Written Employment Equity Plan
Information technology	Hardware Internal company emails Internet Licenses Software packages Telephone lines, leased lines, and data lines
Insurance	Insurance policies

8. PROCESSING OF PERSONAL INFORMATION

8.1 PURPOSE OF PROCESSING PERSONAL INFORMATION

8.1.1 The administration of our business;
8.1.2 supplying our products and/or services to you;
8.1.3 managing payments for our products and/or services;
8.1.4 personalising and tailoring our products and/or services for you;
8.1.5 communicating with you;
8.1.6 historical, research, statistical, and marketing purposes.

8.2 DESCRIPTION OF THE CATEGORIES OF DATA SUBJECTS AND OF THE INFORMATION OR CATEGORIES OF INFORMATION RELATING THERETO

Categories of data subjects	**Personal information that may be processed**
Clients	**Identity information** including, but not limited to, the following: Identity numbers, driving licences, passport numbers, names, surnames, company or entity names and registration details, vehicle registration numbers, CCTV footage, and biometric information such as fingerprint images. **Contact and location information**, including, but not limited to, the following: Telephone and fax numbers, email addresses, physical addresses, postal addresses, and geographical location data.

	Business information including, but not limited to, the following: Ownership, shareholding, job titles, professions, private and/or confidential email communications of an implicit or explicit nature, affiliations, products, services, and statutory registration information. **Payment information** including, but not limited to, the following: Transaction history, bank statements, invoices, credit notes, credit and/or debit card details, bank account numbers, credit ratings. **Profile information** including, but not limited to, the following: Preferences, customer profiles, and transaction history.

8.3 RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL INFORMATION MAY BE SUPPLIED

GNI may provide the personal information of data subjects to its employees and third parties as part of executing its mandate.

8.4 PLANNED TRANSBORDER FLOWS OF PERSONAL INFORMATION

GNI does not transfer or intend on transferring personal information to physical or intangible sources outside the borders of the Republic.

8.5 GENERAL DESCRIPTION OF INFORMATION SECURITY MEASURES TO BE IMPLEMENTED BY THE RESPONSIBLE PARTY TO ENSURE THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF THE INFORMATION

DATA FILES PROTECTION

Data Classification: All data files are categorized into sensitivity levels (e.g., public, internal, confidential, highly confidential). The classification determines the necessary security controls.

Access Control: Access to data files is limited to authorized personnel based on job roles. Permissions are reviewed periodically to ensure they remain appropriate.

Encryption: Data files classified as confidential or highly confidential are encrypted both in transit and at rest. Encryption keys are securely managed and periodically updated.

BACKUP AND OFFSITE STORAGE

Regular Backups: Backups of all critical data files are performed daily to ensure data recovery in the event of loss or corruption.

Offsite Storage: Backup files are stored securely offsite to protect against physical damage or loss. Offsite storage facilities are compliant with industry standards and access is restricted to authorized personnel.

Backup Encryption: All backup data is encrypted to ensure confidentiality and integrity. Encryption keys are managed and rotated securely.

Backup and Recovery: Regular backups of data files are performed to ensure data can be recovered in case of loss or corruption. Backup files are encrypted and stored securely in a separate location.

Physical Security: Physical access to servers and storage devices is restricted to authorized personnel only. Data storage facilities are protected by appropriate security measures.

Data Handling: When transferring or sharing data files, secure methods such as encrypted email attachments or secure file transfer protocols are used. Data files are not stored on personal devices unless encrypted and authorized.

Testing and Recovery: Regular tests of backup restoration procedures are conducted to ensure data can be reliably recovered. The results of these tests are documented and reviewed.

USERNAME AND PASSWORD PROTECTION

Password Policies: Strong password policies are enforced, including minimum length, complexity requirements, and periodic password changes. Users are required to create passwords that include a mix of letters, numbers, and special characters.

Multi-Factor Authentication (MFA): MFA is required for access to sensitive systems and data. Users must authenticate using a second factor in addition to their password.

Password Storage: Passwords are securely hashed and salted in accordance with best practices. Plaintext passwords are never stored.
Account Lockout: Accounts are automatically locked after a specified number of failed login attempts to protect against unauthorized access.

OFFICE 365 EMAIL SERVICES

Email Security: Office 365 email services are configured with advanced security features, including encryption, anti-spam, and anti-phishing protections.

Access Control: Email accounts are protected with strong passwords and MFA. Access to email accounts is restricted based on role and reviewed regularly.

Data Loss Prevention (DLP): DLP policies are implemented within Office 365 to prevent the inadvertent sharing of sensitive information. Alerts and actions are configured to manage potential breaches.

Email Retention: Emails are retained in accordance with the organization's data retention policy and applicable legal requirements. Periodic reviews ensure that outdated emails are securely deleted.

Spam and Phishing Protection: Email systems are equipped with filters to detect and block spam and phishing attempts. Employees are trained to recognize and report suspicious emails.

Email Retention: Emails are retained according to our data retention policy and legal requirements. Periodic reviews and deletions are performed to ensure outdated emails are securely removed.

Confidentiality: Sensitive information should not be included in email communications unless encrypted or securely protected. Confidential information should be communicated using secure channels.

Monitoring and Auditing: Email systems are monitored for unusual activity, and regular audits are conducted to ensure compliance with this policy.

RESPONSIBLE PARTIES

Employees: All employees are responsible for adhering to this policy and promptly reporting any security incidents or breaches.

IT Department: The IT department is tasked with implementing and maintaining security measures for data files, backups, and email systems, including encryption, access control, and monitoring.

Data Protection Officer (DPO): The DPO oversees compliance with data protection laws, provides guidance on data protection practices, and manages data subject requests.