PAIA and POPIA

Manual

Table of Contents

1. Definitions

As per the context of the Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA), the following definitions are applicable:

1.1. "**Data Subject**" means the person to whom personal information relates.
1.2. "**Information Officer**" means the person acting on behalf of the Company and discharging the duties and responsibilities assigned to the "head" of the Company by the Acts; The Information Officer is duly authorised to act as such, and such authorisation has been confirmed by the "head" of the Company in writing;
1.3. "**Personal Information**" means information about an identifiable individual, including, but not limited to information relating to the:
1.3.1. 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;
1.3.2. 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;
1.3.3. any identifying number, symbol or other particular assigned to the individual;
1.3.4. the address, fingerprints, or blood type of the individual;
1.3.5. 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;
1.3.6. 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;
1.3.7. the views or opinions of another individual about the individual;
1.3.8. 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
1.3.9. 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.

2. "**Personnel**" means any person who works for or provides services to or on behalf of the Company and receives or is entitled to receive any remuneration. This includes, without limitation, directors (both executive and non-executive), all permanent, temporary, and part-time staff as well as contract workers.
3. "**Processing**" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:
3.1. The collection, receipt, recording, organisation, collation, storage, updating, modification, retrieval, alteration, or consultation.
3.2. Dissemination by means of transmission, distribution or making available in any other form.
3.3. Merging, linking, as well as restriction, degradation, erasure, or destruction of information.
4. "**Record**" means any recorded information, regardless of form or medium, which is in the possession or under the control of the Company, irrespective of whether it was created by the Company.
5. "**Request**" means a request for access to a record of the Company.
6. "**Requestor**" means any person, including a public body or an official thereof, making a request for access to a record of the Company and includes any person acting on behalf of that person.
7. "**Responsible Party**" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose and means for processing personal information.

8. "**Unique Identifier**" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.
9. **"Artificial Intelligence (AI)"** means computer systems, software, machine learning models, generative AI systems, automated analytical tools, or similar technologies capable of performing tasks that would ordinarily require human intelligence, including but not limited to data analysis, content generation, automation, classification, prediction, summarisation, and decision support.
10. **"Automated Processing"** means any form of processing of personal information performed by automated means, including through artificial intelligence systems, algorithms, or machine-based analysis tools.

2. Introduction

Dire Wolf is committed to the observance of and compliance with the directives of the South African Constitution and national legislation which endorse the key principles of good corporate governance, transparency, and accountability.

The Promotion of Access to Information Act No. 2 of 2000 (PAIA) gives effect to carry out section 32 of the South African Constitution, which focuses on the right to access information i.e. everyone has the right of access to information held by the state or a private body to enforce a culture of transparency and accountability.

Section 51 of PAIA obliges private bodies (including Dire Wolf) to compile a manual to enable a person to obtain access to information held by such private body and stipulates the minimum requirements that the manual must comply with.

This Manual is published in terms of Section 51 of the Promotion of Access to Information Act (PAIA), 2 of 2000, and describes the type of records held by Dire Wolf and the procedures for data subjects to access that information.

As per Section 17 of the Protection of Personal Information Act (POPIA), 2013, a responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

The process of requesting information in terms of the Act is subjected to applicable legislative and/or regulatory requirements, and the applicable request forms are available as Annexures within this manual.

Enquiries, complaints, and requests relating to PAIA and POPIA may be directed to:

The Information Regulator (South Africa)
JD House
27 Stiemens Street
Braamfontein
Johannesburg
2001

Website: www.inforegulator.org.za

Email: inforeg@justice.gov.za
General Enquiries: enquiries@inforegulator.org.za
PAIA Complaints: PAIAComplaints@inforegulator.org.za
POPIA Complaints: POPIAComplaints@inforegulator.org.za

3. Company Details

Dire Wolf Financial Services is a bespoke insurance advisory firm specialising in niche products and bespoke structuring.

MD/CEO:	Arlene Steyl
Contact Detail:	arlene@direwolf.co.za
Operations manager:	Willem Jens
Contact Details:	willem@direwolf.co.za
Information Officer:	Willem Jens
Contact Details:	willem@direwolf.co.za
Company Address:	558 Azzura St Val De Vie Paarl 7646
Company Contact Detail:	021 205 3569
Company Website:	https://direwolf.co.za/

The latest copy of this Manual is available on the Company website, https://direwolf.co.za, and may also be requested from the Information Officer.

4. Company Records

Categories of information held by Dire Wolf, are outlined below:

Company Act	Company registration document Name & Appointment of Directors Share Certificates Board Meeting Minutes Share and statutory Registers Appointment of Auditors
Financial Records	Accounting Records Annual Financial Statements Bank Accounts and statements Asset Registers Debtors / Creditors statements and invoices General Ledgers Invoices Tax Returns
Income Tax	PAYE Records VAT records Skills Development Levies SARS records UIF
Procurement	Supplier Agreements Supplier Lists Policies & Procedures
Personnel	CV's Accident registry Address Lists Disciplinary codes and records Employee benefits Employment contracts Forms and applications Medical aid records Leave records Skills Development Records
Sales	Customer details Advertising material
Information & Communication	Technology Asset Registers User Manuals Software Development Policies & Procedures

	Software Licensing Systems Documentation & Manuals Database systems
Client Information	Client records Consent Forms Financial Detail

5. Records held as per Legislation.

Information is retained in terms of the following legislations and is usually available only to the persons or entities specified in such legislation. Although we have used our best efforts to supply a list of applicable legislation, it is, however, possible that this list may be incomplete.

- Basic Conditions of Employment Act, No. 75 of 1997
- Companies Act, No. 71 of 2008
- Compensation for Occupational Injuries and Diseases Act, No. 130 of 1993
- Constitution of the Republic of South Africa, 1996
- Consumer Protection Act, No. 68 of 2008
- Debtor Collectors Act, No. 114 of 1998
- Electronic Communications and Transactions Act, No. 25 of 2002
- Employment Equity Act, No. 55 of 1998
- Financial Sector Regulation Act, No. 9 of 2017
- Financial Intelligence Centre Act, No. 38 of 2001
- Financial Advisory and Intermediary Services Act, No. 37 of 2002
- Income Tax Act, No. 58 of 1962
- Insurance Act, No. 18 of 2017
- Labour Relations Act, No. 66 of 1995
- Long-term Insurance Act, No. 52 of 1998
- Medical Schemes Act, No. 131 of 1998
- Occupational Health and Safety Act, No. 85 of 1993
- Pension Funds Act, No. 24 of 1956
- Promotion of Access to Information Act, No. 2 of 2000
- Protection of Personal Information Act, No. 4 of 2013
- Short-term Insurance Act, No. 53 of 1998
- Skills Development Levies Act, No. 9 of 1999
- Tax Administration Act, No. 28 of 2011
- Unemployment Contributions Act, No. 4 of 2002
- Unemployment Insurance Act, No. 63 of 2001
- Value-Added Tax Act, No. 89 of 1991

6. Protection of Personal Information

Dire Wolf is capturing, processing, storing, and communicating Personal Information to perform its business functions. Dire Wolf acts as a Responsible Party and is accountable for ensuring that the Personal Information of Data Subjects is:

- processed lawfully, fairly, and transparently.
- processed only for the purposes for which it was collected.
- will not be further processed in a manner incompatible with the purpose for which it was collected, unless otherwise permitted by applicable legislation.
- is accurate and kept up to date and will not be kept for longer than necessary.
- 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, is subject to an appropriate level of security when stored, processed, and communicated.
- processed in accordance with the rights of Data Subjects, where applicable.

Dire Wolf may utilise approved Artificial Intelligence ("AI") technologies and automated processing systems to support operational efficiency, administrative processing, customer communication, compliance monitoring, fraud detection, analytical activities, reporting, and service delivery. Any use of AI involving Personal Information shall be subject to appropriate security, confidentiality, governance, oversight, and access control measures in accordance with applicable legislation and company policies.

Dire Wolf will take reasonable steps to ensure that Personal Information processed through AI systems or third-party technology providers is processed lawfully, securely, and only for authorised business purposes.

Personal Information will not knowingly be uploaded into publicly accessible AI platforms unless appropriate safeguards, approvals, and contractual protections are in place.

7. Rights of Data Subjects

Data subjects have the following rights:

- To be notified that their Personal Information is being collected.
- To be notified in the event of a data breach.
- To enquire whether Dire Wolf holds Personal Information about them and, where applicable, to request access to such information in accordance with PAIA and POPIA. Any request for information must be handled in accordance with the provisions of this Manual.
- To object, on reasonable grounds relating to their particular situation, to the processing of their Personal Information where permitted by law.
- To request the correction, destruction, or deletion of Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully, subject to applicable legal, regulatory, contractual, and record retention obligations
- To object to the processing of Personal Information for purposes of direct marketing by means of unsolicited electronic communications.
- To 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 noncompliance with the protection of his, her or its personal information.

Data Subjects may enquire about the manner in which their Personal Information is processed, including whether automated processing technologies or Artificial Intelligence ("AI") systems materially contribute to such processing, subject to applicable legal, regulatory, security, confidentiality, and commercial limitations.

8. Information security measures

Dire Wolf is committed to protecting the integrity, availability, and confidentiality of Personal Information in its possession and under its control through the implementation of appropriate technical, organisational, and administrative security measures.

Dire Wolf maintains a risk-based information security framework designed to identify, assess, manage, and monitor information security risks. Security controls are selected and implemented based on the nature of the information processed, applicable legal and regulatory requirements, industry best practices, and the operational requirements of the business.

Information security controls are implemented and monitored as part of Dire Wolf's Information Security Management System and are guided by the organisation's Information Security Charter, which establishes the information security objectives of the organisation. The Information Security Policy further directs the rules, policies, standards, and procedures necessary to protect information assets, systems, networks, and users.

Security measures implemented by Dire Wolf may include, but are not limited to:
- access controls, authentication measures, and user access management for systems containing Personal Information;
- monitoring, approval, and governance of third-party cloud, software, and Artificial Intelligence ("AI") platforms used within the organisation;

- employee awareness, training, and acceptable-use requirements relating to confidential information, Personal Information, and AI technologies;
- data minimisation principles designed to limit the unnecessary collection, processing, disclosure, and retention of Personal Information;
- physical, technical, and organisational safeguards to protect information against unauthorised access, disclosure, alteration, destruction, loss, or misuse;
- monitoring and review processes to assess the effectiveness of security controls and identify areas for improvement; and
- incident management and breach response processes designed to identify, contain, investigate, and address information security incidents.

Dire Wolf will take reasonable steps to ensure that all employees, contractors, service providers, and authorised users who have access to Personal Information understand and comply with applicable information security requirements.

Artificial Intelligence and Automated Processing

Dire Wolf acknowledges the increasing use of Artificial Intelligence ("AI") and automated technologies within business operations and is committed to ensuring that such technologies are used responsibly, securely, and in compliance with applicable legislation, regulatory obligations, and internal policies.

AI systems and automated processing technologies may be utilised to support operational efficiency, reporting, communications, workflow automation, analytical activities, fraud detection, customer service functions, document drafting, compliance monitoring, administrative processes, and other legitimate business purposes.

Dire Wolf will implement reasonable controls to manage risks associated with the use of AI technologies, including but not limited to:
- restricting the upload of Personal Information, confidential information, or sensitive business information into unapproved AI platforms;
- ensuring appropriate human oversight of AI-generated outputs, recommendations, and decisions where required;

- limiting access to approved systems and authorised personnel only;
- monitoring service providers and third-party platforms that process Personal Information on behalf of Dire Wolf;
- implementing reasonable technical and organisational security measures to protect Personal Information processed through AI-enabled systems;
- maintaining governance processes relating to the assessment, approval, implementation, and use of AI technologies; and
- requiring users of AI systems to review and validate AI-generated outputs before such outputs are relied upon for operational, customer, compliance, or business purposes.

Where AI systems are provided by third-party service providers or cloud-based platforms, Dire Wolf will take reasonable steps to ensure that such providers maintain appropriate technical, organisational, contractual, and security safeguards for the protection of Personal Information.

Where Personal Information is processed by AI platforms or technology providers outside the Republic of South Africa, Dire Wolf will take reasonable steps to ensure that such processing is conducted in accordance with applicable cross-border information transfer requirements and the provisions of the Protection of Personal Information Act, No. 4 of 2013.

AI systems utilised by Dire Wolf are intended to support human decision-making and operational processes and are not intended to replace appropriate human oversight, professional judgement, professional advice, or regulatory compliance obligations

9. Request for information

In terms of PAIA and POPIA, a Data Subject may, upon providing adequate proof of identity, request confirmation as to whether Dire Wolf holds Personal Information relating to them. A Data Subject may also request access to such Personal Information, including information relating to the identity of third parties who have, or have had, access to such information, where applicable and permitted by law.

A Data Subject may object to the processing of their Personal Information where permitted by applicable legislation. Requests for access to records or Personal Information held by Dire Wolf must comply with the procedural requirements prescribed by PAIA and POPIA.

To request access to information or records, the prescribed Form 02: Request for Access to Record must be completed and submitted to the Information Officer together with any supporting documentation and applicable fees, where required. The prescribed time periods for processing a request will commence once all required information and supporting documentation have been received.

The Information Officer will consider each request in accordance with the provisions of PAIA and POPIA and may grant access only to records or portions of records that are not prohibited from disclosure by applicable legislation. Dire Wolf will process requests within the time periods prescribed by applicable legislation and will communicate the outcome of the request in writing. Where permitted by law, the applicable response period may be extended, and the requester will be notified accordingly.

The process to request information from Dire Wolf is as follows:

- The prescribed Form 02: Request for Access to Record must be completed in full and submitted to file a request for access to a record.
- If an individual is unable to complete the prescribed form due to illiteracy, disability, or any other reasonable cause, such person may make the request orally, and the Information Officer will assist in reducing the request to writing where required.
- An application for access to information may be refused if it does not comply with the requirements of PAIA. If access to a record or information is denied, the requester will be notified in writing and provided with adequate reasons for the refusal, subject to any legal limitations on the disclosure of such reasons.
- Should the requester not be satisfied with the decision of the Information Officer, the requester may lodge a complaint with the Information Regulator or apply to a court for appropriate relief in accordance with the provisions of PAIA.
- Dire Wolf will require proof of identity from the Data Subject or requester. Where a request is submitted on behalf of another person, proof of authority to act on behalf of that person may also be required.
- The successful completion and submission of a request for access does not automatically entitle the requester to access the requested records.
- If access to a record or information is granted, the requester will be notified accordingly and advised of any applicable access fees payable before access is provided.

10. Objection to the Processing of Personal Information

Section 11(3) of the Protection of Personal Information Act, No. 4 of 2013 ("POPIA"), provides that a Data Subject may, on reasonable grounds relating to their particular situation, object to the processing of their Personal Information by Dire Wolf, unless such processing is required or authorised by law.

Any objection to the processing of Personal Information must be submitted to the Information Officer using the prescribed form and will be considered and processed in accordance with the provisions of POPIA and any other applicable legal or regulatory requirements.

11. Request for correction or deletion of Personal Information

Section 24 of POPIA and the applicable POPIA Regulations provide that a Data Subject may request that their Personal Information be corrected or deleted by submitting the prescribed form.

To ensure the accuracy, completeness, and lawfulness of Personal Information, a Data Subject may request Dire Wolf to correct or delete Personal Information in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully.

A Data Subject may also request Dire Wolf to destroy or delete a record containing Personal Information that Dire Wolf is no longer authorised to retain in terms of POPIA and applicable record retention requirements.

Any request for the correction, deletion, destruction, or restriction of Personal Information will be considered and processed in accordance with the provisions of POPIA and any other applicable legal or regulatory obligations.

12. Fees

Where Dire Wolf has made categories of records available automatically, the only fee that may be charged for access to such records is a reasonable reproduction fee, where applicable.

PAIA provides for two types of fees, namely a request fee and an access fee.

A request fee is a non-refundable administrative fee payable by a requester, other than a personal requester, before a request for access to a record will be processed. The applicable request fee will be determined in accordance with the fees prescribed under PAIA and its regulations.

An access fee may be payable where access to a requested record is granted. The access fee is intended to reimburse Dire Wolf for the costs associated with searching for, preparing, reproducing, and providing access to the requested record.

Where applicable, the requester will be notified of any fees payable before access to the requested record is provided.

Dire Wolf may withhold access to a requested record until any applicable fees prescribed by PAIA have been paid.

All fees charged in relation to requests for access to records will be determined in accordance with the provisions of PAIA and the applicable regulations in force from time to time.

Item for Reproduction and/or Access
Fee (ZAR)

Item	Description	Amount
1.	Request fee, payable by every requester	R140.00
2.	Photocopy or printed black & white copy for every A4 page	R2.00 per page or part of the page
3.	Printed copy of A4-size page	R2.00 per page or part of the page
4.	For a copy in a computer-readable form on: • a flash drive (provided by the requester) • a compact disc (CD) if the requester provides the CD to us • a compact disc (CD) if we give the CD to the requester	R40.00 R40.00 R60.00

Item	Description	Amount
5.	For a transcription of visual images, for an A4-size page or part of the page	This service will be outsourced. The fee will depend on the quotation from the service provider.
6.	For a copy of visual images	This service will be outsourced. The fee will depend on the quotation from the service provider.
7.	For a transcription of an audio record, per A4-size page	R24.00
8.	For a copy of an audio record on a flash drive (provided by the requester) For a copy of an audio record on compact disc (CD) if the requester provides the CD to us For a copy of an audio record on compact disc (CD) if we give the CD to the requester	R40.00 R40.00 R60.00
9.	For each hour or part of an hour (excluding the first hour) reasonably required to search for, and prepare the record for disclosure The search and preparation fee cannot exceed	R145.00 R435.00
10.	Deposit: if the search exceeds 6 hours	One-third of the amount per request. It is calculated in terms of items 2 to 8 above.
11.	Postage, email or any other electronic transfer	Actual expense, if any.