




NKWE PLATINUM GROUP

PRIVACY

POLICY

APPROVAL SIGNATURE RECORD				
#	NAME AND SURNAME	ROLE	SIGNATURE	DATE
1.	Claire Rutenberg	Policy Originator & Administrator		2025/07/16
2.	Vikesh Dhanooklal	Policy Reviewer		2025-07-16
3.	Hongzhang (Leon) Yang	Policy Approver		2025-09-16
4.				
5.				

Document number	Revision number	Effective date
POL-RCM-001	000	July 2025

TABLE OF CONTENTS

1. INTRODUCTION, PURPOSE, AND SCOPE	3
1.1 INTRODUCTION	3
1.2 PURPOSE AND SCOPE.....	3
2. DESCRIPTION OF REVIEW / REVISION.....	4
3. TERMS, ABBREVIATIONS AND DEFINITIONS.....	4
4. ROLES AND RESPONSIBILITIES	7
4.1 POLICY OWNER.....	7
4.2 POLICY ADMINISTRATOR	8
4.3 EMPLOYEES	8
4.4 MANAGERS.....	8
4.5 CONTRACTOR / CONSULTANT	8
4.6 HUMAN RESOURCES MANAGER OR DULY APPOINTED NOMINEE	8
4.7 INFORMATION OFFICER / DEPUTY INFORMATION OFFICER	8
4.8 EXECUTIVE COMMITTEE.....	9
5. REGULATORY ASPECTS	10
6. BUSINESS PROCESS ASPECTS.....	10
6.1 ABOUT THE COMPANY	10
6.2 PURPOSE OF COLLECTING & PROCESSING PI	10
6.3 LAWFUL BASIS.....	11
6.4 PERIOD OF HOLDING PERSONAL INFORMATION.....	12
6.5 DATA SUBJECTS RIGHTS	12
6.6 SOURCES OF PI.....	12
6.7 CATEGORIES OF PI COLLECTED & PROCESSED	13
6.8 DISCLOSURE OF INFORMATION.....	14
6.9 INFORMATION SECURITY	14
6.10 DIRECT MARKETING.....	15
7. COMMUNICATION AND IMPLEMENTATION	15
8. RELATED DOCUMENTS / POLICIES.....	15
9. DELEGATIONS OF AUTHORITY.....	16
10. CHANGES TO THE POLICY	16
11. CONTACT US.....	16
12. APPENDICES	16

1. INTRODUCTION, PURPOSE, AND SCOPE

1.1 INTRODUCTION

The company is committed to protecting data subject privacy as well as ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws. This is in line with the Constitutional provisions.

The Protection of Personal Information Act 4 of 2013 requires the company to inform its data subjects as to how their personal information is collected, processed, secured, disclosed, and destroyed.

The provisions of this policy must be read along with the relevant practices and procedures that are used to operationalise the purpose hereof.

1.2 PURPOSE AND SCOPE

The purpose of this policy is to advise the data subject and/or the Operator why personal information is collected and processed, what data is in focus as well as how it is processed. The Company is committed to compliance with the Protection of Personal Information Act insofar as the utilisation and disclosure of personal information is concerned. Technical and organisational measures have been put in place to protect data subject privacy, and the Company invites all data subjects and/or requesters to engage with its Information Officer / Deputy Information Officer in respect of any matter related hereto.

This policy applies to data subjects under the Protection of Personal Information Act and its principles extend to the Promotion of Access to Information Act 2 of 2000 in respect of requesters of records held by the Company. PI applies to both natural and juristic persons. Data subjects and requesters are invited to engage with the Information Officer / Deputy Information Officer about any matter pertaining to the Protection of Personal Information Act, including but not limited to updating PI, deleting of PI, complaints in respect of how PI is being processed and updating consent for electronic direct marketing.

This policy applies to all personal information processed by the Company whether electronic or non-electronic format. It extends to all employees, clients, suppliers, and other data subjects / stakeholders whose personal information is processed by the Company.

2. DESCRIPTION OF REVIEW / REVISION

REV.NO.	PAGE	DETAILS	EFFECTIVE DATE	REVIEWED BY

3. TERMS, ABBREVIATIONS AND DEFINITIONS

TERM / ABBREVIATION	DEFINITION
CRM	Customer Relationship Management.
Data Subject	The person to whom personal information relates to.
DIO	Deputy Information Officer.
IO	Information Officer.
IRL	Incident Response Lead.
Operator	A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
Person	A natural person or a juristic person.

TERM / ABBREVIATION	DEFINITION
Personal Information	<p>Information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to-</p> <ul style="list-style-type: none"> (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.
PI	Personal Information.
PAIA	Promotion of Access to Information Act 2 of 2000.
POPIA	Protection of Personal Information Act (Act No. 4 of 2013).
Private Body	<ul style="list-style-type: none"> (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.

TERM / ABBREVIATION	DEFINITION
Processing	<p>Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including-</p> <ul style="list-style-type: none"> (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.
Public Body	<ul style="list-style-type: none"> (a) Any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when- <ul style="list-style-type: none"> i) exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or ii) exercising a public power or performing a public function in terms of any legislation.
Regulator	The Information Regulator established in terms of Section 39 of the POPIA.
Responsible Party	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.
Record	<p>Of, or in relation to a public or private body, means any recording information –</p> <ul style="list-style-type: none"> (a) regardless of form or medium; (b) in the possession or under control of that public or private body, respectively; and (c) whether or not it was created by the that public or private body, respectively;

TERM / ABBREVIATION	DEFINITION
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.
Third Party	In relation to a request for access to – (a) a record of a public body, means any person (including but not limited to, the government of a foreign state, an international organisation or an organ of government or organisation) other than – i) the requester concerned; and ii) a public body; or (b) a record of private body, means any person (including but not limited to, a public body) other than the requester, but, for the purposes of sections 34 and 63, the reference 'person' in paragraphs (a) and (b) must be construed as a reference to 'natural person';
The Act	Means the Promotion of Access to Information Act 2 of 2000 as amended, and includes any regulation made and in force in terms of section 92.
The Company	Nkwe Platinum Limited (incorporated in Bermuda) and registered as an external company in South Africa and its wholly owned subsidiary - South Africa Zijin Platinum (Pty) Limited.

4. ROLES AND RESPONSIBILITIES

4.1 POLICY OWNER

The policy owner is responsible for coordinating, from the functional owner perspective, the activities relating to originating, reviewing and roll out activities as defined in the policy life cycle process.

The policy owner is responsible to retain appropriate documentation as to respective steps to approval and rollout of the policy in the designated policies working folder.

Policy owners also responsible for considering the main areas of risk, the specific relevance given, as well as the structure and life stage of the organization, the approach to address those, the related controls, and the specific policies to formalize or put in place.

This privacy policy outlines how the Company will collect, use, disclose, and protect personal information in accordance with the Protection of Personal Information Act (POPIA) and other relevant legislation.

4.2 POLICY ADMINISTRATOR

The policy administrator coordinates the policies process and governance aspects regarding the respective life cycle of policies until approval and is responsible for the publication of the document in the policies repository and register.

The policy administrator also maintains the policies register.

4.3 EMPLOYEES

Employees are responsible to familiarize themselves with the policy within 48 hours from publication and to log any queries or questions for clarity regarding the policy via e-mail with the Policy Owner and, for record purposes, copy the Policies Administrator.

4.4 MANAGERS

Managers shall support the roll-out and enforcement of adherence to the implementation and compliance of policies and procedures. Managers are also responsible for appropriately addressing instances of non-compliance, including notice to the relevant policy owner and to coordinate with the Human Resource Department to ensure appropriate process as to disciplinary aspects of the governance framework.

4.5 CONTRACTOR / CONSULTANT

Contractors and consultants are required to comply with the Policy while providing their services to the Company. This Policy is equally applicable to them and requires their full compliance to it.

4.6 HUMAN RESOURCES MANAGER OR DULY APPOINTED NOMINEE

To ensure that the employment contracts, recruitment procedures and employee records are in line with this Policy.

4.7 INFORMATION OFFICER / DEPUTY INFORMATION OFFICER

The Information Officer / Deputy Information Officer shall ensure that all departments comply with this policy, in accordance with POPIA and as laid out within the Company's POPIA Policy.

Information Officer details:

Name: Hongzhang Yang
Telephone number: 010 591 3989
Postal address: PostNet Suite #316
Private Bag X29
Gallo Manor
2052
Physical address: Woodlands Office Park
2nd Floor, Building 18
20 Woodlands Drive
Woodlands
Sandton
2191
Email address: lyang@zijinplatinum.co.za

Deputy Information Officer details:

Name: Claire Rutenberg
Telephone number: 010 591 3989
Postal address: PostNet Suite #316
Private Bag X29
Gallo Manor
2052
Physical address: Woodlands Office Park
2nd Floor, Building 18
20 Woodlands Drive
Woodlands
Sandton
2191
Email address: crutenberg@zijinplatinum.co.za

The list of records that are voluntarily disclosable and/or available without a requester having to request access thereto shall be kept and updated monthly and/or whenever the contents change. The said list shall be posted on the website, registered with the Information Regulator, and kept in hard copy at the offices of the company.

4.8 EXECUTIVE COMMITTEE

The executive committee oversees the governance process and approves appropriate policies in executing responsibilities and reports to the board of directors.

5. REGULATORY ASPECTS

We base our actions on compliance with the laws, rules, and regulations. The Code is based on the cardinal idea of legal compliance, both in letter and in spirit. All individuals must respect and obey the laws of South Africa and avoid even the appearance of impropriety.

The company is obliged to comply with the Protection of Personal Information Act (No. 4 of 2013) ("POPIA") as well as the Promotion of Access to Information Act (No. 2 of 2000) ("PAIA"), given that it processes the personal information of its employees, suppliers, clients, and other data subjects from time to time as well as consideration that there may be requesters of information relating to the company and its operations.

It is a requirement of POPIA to adequately protect the personal information that the company holds and to avoid unauthorised access and use of personal information.

The company shall review its technical and operational security controls and processes on a regular basis to ensure that personal information is secure.

6. BUSINESS PROCESS ASPECTS

6.1 ABOUT THE COMPANY

The Company owns and operates the Zijin Garatau Platinum Mine is currently under construction, and will be an underground operation, mining Platinum Group Metals (PGM's) and all associated minerals. The mining right covers the farms: De Kom 252KT, Hoepakrantz 291KT, Portion 1 and the Remaining Extent of the farm Garatouw 282KT, with certain surface infrastructure on a portion of the farm Maandagshoek 254 KT. The Mine is situated within the jurisdiction of Fetakgomo, Tubatse and Makhuduthamaga Local Municipalities in Sekhukhune District Municipality, Limpopo Province.

More details in this regard can be obtained on the "HOME" page on its website.

6.2 PURPOSE OF COLLECTING & PROCESSING PI

The Company processes PI for various purposes including for –

- Facilitating transactions with data subjects.
- Collecting data for statistical purposes to improve its services.
- Fulfilling its contractual obligations to its clients and client contacts.
- Complying with the provisions of statute and regulations.
- Attending to the legitimate interests of data subjects.
- Identifying prospects for enhanced service delivery and business sustainability.

- Tracking data subject activity on the website and its links as well as their transactions with the Company.
- Providing data subject information to the Company partners, to use the information to market their services to data subjects who are current clients and/or who have consented as envisaged in the POPIA. These partners who are recipients of PI are business organizations who are permitted to use the information only for lawful sales, marketing, and engagement.
- Confirm and verify data subject identity or to verify that they are authorised users for security purposes.
- Conduct market or customer satisfaction research, where consent has been obtained.
- Audit and record keeping purposes.
- In connection with legal proceedings.
- The Company may also collect personal information from third parties were permitted by law.
- Recruitment and employment purposes.
- To transact and run the business of the Company in accordance with the law and practice.

6.3 **LAWFUL BASIS**

In respect of the processing of PI as provided for herein, the Company will adhere to the conditions for the lawful processing of PI, based on its desire to provide data subjects services in their best interests as well as a legitimate interest of the Company to achieve its business objectives, including acquiring the Data Subjects consent. In addition, where personal information is transmitted across South African borders, the Company will ensure that the destination country and organisation has protections similar to those of POPIA. Furthermore, where special personal information is processed, including under 18-year-old data subjects, consent from the Information Regulator and/or competent persons will be obtained as required.

The Company will only process personal information where the Company has a lawful basis to do so. The lawful basis the Company relies on includes:

- a) Consent of the data subject.
- b) Processing is necessary for the performance of a contract.
- c) Compliance with legal obligations.
- d) Legitimate interests pursued by the Company or a third party.

6.4 PERIOD OF HOLDING PERSONAL INFORMATION

The Company will use personal information for the purpose intended and this includes that it will attempt to keep the personal information up to date. It will be the data subject's responsibility to ensure that they keep the Company updated on their P.I. The Company shall keep records of personal information for as long as it is required at law as a minimum and will regularly evaluate whether it should thereafter be destroyed or de-identified.

Each department is required to keep all records stored in a safe and secure manner. When a document/data is no longer required or a data subject requests its disposal, the Head of the Department or duly assigned personnel, is required to dispose/delete said data/documentation and provide a response back to the data subject with evidence of the data/documentation's destruction where possible.

6.5 DATA SUBJECTS RIGHTS

Data Subjects have the right to request access to any personal information that the company holds about them.

Data Subjects have the right to request the Company to update, correct or delete their personal information on reasonable grounds. Such requests must be made to the company's Information Officer / Deputy Information Officer (see clause 5), to the Company's head office (see details below).

Where an employee or client objects to the processing of their personal information, the Company may no longer process said personal information. The consequences of the failure to give consent to process the personal information must be set out before the employee or client confirms their objection.

The data subject must provide reasons for the objection to the processing of their personal information.

Data subjects have the right to request that the Company provide them with access to their PI, to rectify or correct their personal information, erase PI, or restrict the processing of PI, including refraining from sharing it or otherwise providing it to any third parties. Data subjects also have the right to raise complaints with the Information Regulator.

The afore-going rights may be subject to certain limitations pursuant to applicable law. In order to access any of these rights, the data subject may contact the Information Officer / Deputy Information Officer.

6.6 SOURCES OF PI

The Company gathers PI from several sources, which include directly from data subjects, publicly available sources such as websites, social media, commercial transactions with the Company, referrals, prospects, partner agreements, training engagements, conferences, and the like. Given that PI can be extracted and/or obtained from several sources and consolidated into one CRM or other similar systems of record, it may be difficult or impossible to identify the exact source of one particular piece of information.

6.7 CATEGORIES OF PI COLLECTED & PROCESSED

The Company collects information about data subjects that are part of its scope of operations.

Depending on the purpose of the transaction, some, or all of the following categories of personal information on data subjects, historical or current, may be processed –

- Name and surname
- Identity / passport number
- Race, gender & disability status
- Citizenship, Visa's, and work permits
- Contact details (email, mobile, postal address)
- Birth date
- Banking details
- Criminal, credit, reference or similar checks and reports
- Benefits covered by or through the Company
- Medical information such as diagnoses, allergies, or work restrictions due to health
- Certificates and qualifications
- Position held and responsibilities
- Areas of interest in respect of the Company offerings
- Record of services used
- Email correspondence and attachments
- Organisation details
- Office address
- Office contact details
- Organisation email Address
- Organisation and data subject social media URL's
- Remuneration and tax information
- Emergency contact information
- Disciplinary and performance records
- Biometrics (Facial and fingerprints)
- Service providers and operators processing information on the Company's behalf
- Professional advisors and consultants
- Regulatory authorities and government agencies
- Other information that is available in the public domain.

We collect and process personal information mainly to contact data subjects for the purpose of understanding their requirements and delivering services accordingly. Where possible, we will inform data subjects what information they are required to provide to the Company and what information is optional, as well as the consequences of not providing the said information.

Website usage information may be collected using “cookies” which allows the Company to collect standard internet visitor usage information.

6.8 DISCLOSURE OF INFORMATION

The Company may disclose data subject PI to its third-party service providers, after obtaining consent from the data subjects, who are involved in the delivery of products or services data subjects. The Company has agreements in place to ensure that it complies with the privacy requirements as required by the POPI Act.

The Company may also disclose data subject PI:

- Where it has a duty or a right to disclose in terms of law and/ or industry codes;
- Where it believes it is necessary to protect its rights.
- Service providers and operators processing information on the Company's behalf
- Professional advisors, consultants and contractors
- Providing data subject information to the Company's business partner/s; and its holding company - Zijin Mining Group.
- Regulatory authorities and government agencies

When transferring personal information, we ensure appropriate safeguards are in place to protect the information.

6.9 INFORMATION SECURITY

The Company is legally obliged to provide adequate systems, technical and organisational protection for the PI that it holds and to prevent unauthorized access to as well as prohibited use of PI. It will therefore, on a regular basis, review its security controls and related processes to ensure that the PI of data subjects remains secure.

The Company has conducted an impact assessment across all of its functions and used the findings thereof to manage risk optimally as well as to provide iterative improvements on an ongoing basis. The Company policies and procedures cover the following aspects –

- Physical security;
- Computer and network security;
- Access to personal information;
- Secure communications;

- Security in contracting out activities or functions;
- Retention and disposal of information;
- Acceptable usage of personal information;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

The Company also ensures that it contracts with Operators as required by POPIA and it requires appropriate security, privacy, and confidentiality obligations of these Operators in order to ensure that personal information is kept secure. The same protocols apply to any party to whom the Company may pass PI on to for the purposes mentioned herein.

6.10 DIRECT MARKETING

The Company will only use personal information for direct marketing purposes where the data subject/s have given consent to use and re-use, publish, distribute, and/or broadcast the Media, in whole or in part, individually or in conjunction with other photographs, images, videos, text, quotes, summaries, biographies, and or excerpts of (collectively called the "Media"), in any and all promotional, educational, business, trade, advertising, and marketing materials, including, but not limited to, in connection with company promotional activities.

7. COMMUNICATION AND IMPLEMENTATION

The policy is published on the Policies platform accessible by all staff and announced to all staff via e-mail, noting that staff are to immediately engage with line managers or Policy Owner should any clarification be required. Approval and implementation of the Policy is also announced during the recurring management meetings, creating the opportunity for any questions for clarification or feedback regarding the policy and the related business process.

The Policy owner will arrange training and knowledge sharing sessions with key stakeholders as and when needed.

8. RELATED DOCUMENTS / POLICIES

Related documents / policies as per order of reference within this policy:

Document Type	Document No.	Document Name
POL	POL-IT-004	Information Security
POL	POL-XRP-002	Social Media Policy
POL	POL-PRO-001	Purchasing Policy
Manual	-	PAIA Manual

9. DELEGATIONS OF AUTHORITY

The Company's directors and management are required to set out the policy and procedure requirements and obligations as per relevant international and local legislative requirements.

Managers key responsibilities are to ensure that they along with all employees, and applicable independent contractors / consultants adhere to the policy requirements and escalate any issues that may be presented.

Employees, and applicable independent contractors / consultants are responsible for ensuring compliance with this policy and reporting any suspected behaviour that may be in contravention of the guidelines set out within this policy.

10. CHANGES TO THE POLICY

The Company may update this Privacy Policy from time to time to reflect changes in the Company practices or legal requirements. The Company will notify data subjects of any material changes and obtain consent where required.

11. CONTACT US

If a Data Subject has any complaints about the Company processing of personal information, please contact the Company Information Officer or Deputy Information Officer. Data Subjects also have the right to lodge a complaint with the information regulator: [eservices: Information Regulator \(infoeregulator.org.za\)](mailto:eservices@informationregulator.org.za).

12. APPENDICES

None.