PAIA (PROMOTION OF ACCESS TO INFORMATION) MANUAL

&

POPI (PROTECTION OF PERSONAL INFORMATION) MANUAL

O F

ZAK STEEL PROPRIETARY LIMITED

(herein referred to as "ZAK STEEL")

COMPANY REGISTRATION NUMBER:

2003/015241/07

REGISTERED OFFICE:

4 Boniface Road, Selection Park Industrial Sites, Springs,

Gauteng, 1559

Prepared in accordance with Section 51 of the Promotion of Access to Information Act, No.2000 and to address the requirements of the Protection of Personal Information Act, 2013.

A copy of the manual is available for inspection at the Company.

PREAMBLE

The Promotion of Access to Information Act No. 2 of 2000, ('PAIA') came into operation in November 2001. Section 51 of this Act requires that Zak Steel, as a private body, compile a manual giving information to the public regarding the procedure to be followed in requesting information from Zak Steel for the purposes of exercising or protecting rights.

On request, the private body or government is obliged to release such information unless the PAIA expressly states that the records containing such information may or must not be released.

The Protection of Personal Information Act, 2013 (the "POPI Act") provides for:

1. The protection of Personal Information[1] processed by public and private bodies;
2. certain conditions so as to establish minimum requirements for the processing of Personal Information;
3. the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of the POPI Act and the PAIA;
4. the issuing of codes of conduct;
5. the rights of persons regarding unsolicited electronic communications and automated decision making;
6. the regulation of the flow of Personal Information across the borders of the Republic; and
7. matters connected therewith.

Section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy. The right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information.

The POPI Act is intended to promote the right to privacy while maintaining the flow of information and enhancing the right of access to and the protection of personal information.

Zak Steel endorses the spirit of the PAIA and POPI Act and believes that this Manual will assist requesters in exercising their rights. The Act seeks, inter alia, to give effect to the constitutional right of access to any information held by the state or by any other person where such information is required for the exercise or protection of any right.

IMPORTANT DEFINITIONS[1]

1. **'biometrics''** means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;
2. **''child''** means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

[1] Section 1 of the Protection of Personal Information Act, No 4 of 2013.

3. **"code of conduct"** means a code of conduct issued in terms of Chapter 7**;**
4. **"competent person"** means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;
5. **"consent"** means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;
6. **"Constitution"** means the Constitution of the Republic of South Africa, 1996;
7. **"data subject"** means the person to whom personal information relates;
8. **"de-identify",** in relation to personal information of a data subject, means to delete any information that—
    a. identifies the data subject;
    b. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
    c. can be linked by a reasonably foreseeable method to other information that identifies the data subject and **"de-identified"** has a corresponding meaning;
9. **"direct marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –
    a. promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
    b. requesting the data subject to make a donation of any kind for any reason;
10. **"electronic communication"** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;
11. **"enforcement notice"** means a notice issued in terms of section 95 of the POPI Act;
12. **"filing system"** means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;
13. **"information matching programme"** means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;
14. **"information officer"** of, or in relation to, a—
    a. **"public body**" means an information officer or deputy information officer as contemplated in terms of section 1 or 17 of the POPI Act; or
    b. **"private body**" means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;
15. **"Information Regulator"** means an independent body established in terms of section 39 of the Protection of Personal Information Act 4 of 2013. It is subject only to the law and the constitution and it is accountable to the national assembly;
16. **"Minister"** means the Cabinet member responsible for the administration of justice;
17. **"operator"** means 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;
18. **"person"** means a natural person or a juristic person;

19. **"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;
20. **"prescribed"** means prescribed by regulation or by a code of conduct;
21. **"private body"** means—
    a. a natural person who carries or has carried on any trade, business or
    b. profession, but only in such capacity;
    c. a partnership which carries or has carried on any trade, business or profession; or
    d. any former or existing juristic person, but excludes a public body;
22. **"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;
23. **"professional legal adviser"** means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;
24. **"Promotion of Access to Information Act"** means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) ("POPI Act");
25. **"public body"** means-
    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—

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;

26. **''public record''** means a record that is accessible in the public domain, and which is in the possession of or under the control of a public body, whether or not it was created by that public body;
27. **''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 any thing 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;
28. **''Regulator''** means the Information Regulator established in terms of section 39;
29. **''re-identify''** in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—
    a. identifies the data subject;
    b. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
    c. can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ''re-identified'' has a corresponding meaning;
30. **''Republic''** means the Republic of South Africa;
31. **''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;
32. **''restriction''** means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;
33. **''special personal information''** means personal information as referred to in section 26;
34. **''this Act''** includes any regulation or code of conduct made under this Act; and
35. **''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.

SECTION A - OUR DETAILS AND CONTACT PERSON

The person responsible for the administration, of and compliance with the Act, has been delegated by the Managing Director. The Designated Information Officer has been registered, the details of which appear herein below.

Requests pursuant to the provisions of the Act should be directed as follows:

Full name	Zak Steel Proprietary Limited
Registration Number	2003/015241/07
Registered address	4 Boniface Road Selection Park Industrial Sites Springs Gauteng 1559
Postal Address	PO Box 747 Springs Gauteng 1560
Telephone Number	+27 11 815 5043
Designated Information Officer	Michael Van Loggerenberg mj@clydeind.co.za
Website	www.zak.co.za

SECTION B - HUMAN RIGHTS COMMISSION (HRC) GUIDE - INFORMATION REGULATOR

The Human Rights Commission was tasked with the administration of the PAIA. Section 10 of the PAIA required the South African Human Rights Commission (SAHRC) to publish a guide which is intended to assist users in the interpretation of the PAIA and how to access the records of private and public bodies and the remedies available in law regarding a breach of any of the provisions of the PAIA.
The guide contained the following information:

1. The objects of the Act;
2. Particulars of the information officer of every public body;
3. Particulars of every private body as are practicable;
4. The manner and form of a request for access to information held by a body;
5. Assistance available from both the information officers and the SAHRC in terms of this Act;
6. All remedies in law regarding acts, omissions, rights and duties, including how to lodge an internal appeal and a court application;
7. Schedules of fees to be paid in relation to requests for access to information;
8. Regulations made in terms of the Act.

With effect from 1 July 2021, the responsibility to fulfil the duties, functions and roles as defined in the PAIA were transferred to the Information Regulator. Copies of this guide are available from SAHRC and / or the Information Regulator. Enquiries regarding the Guide and relating to the person's rights and in particular their right to access information from a private or public body can be addressed to the Information Regulator the contact details of which are as follows:

Contact person	Information Regulator: PAIA (Promotion of Access to Information Act).
Telephone Number	010 023 5200
Email	enquiries@inforegulator.org.za
Website	https://justice.gov.za/inforeg/

SECTION C - INFORMATION AVAILABLE IN TERMS OF THE ACT

Policy regarding confidentiality and access to information

Zak Steel undertakes to protect the confidentiality of information provided to it by its clients, staff and third parties, subject to its obligations to disclose information in terms of any applicable law or regulation or a court order requiring disclosure of information.

If access is requested to a record that contains information about a data subject, Zak Steel is obliged to attempt to contact such data subject to inform him/her/it of the request.

Zak Steel will give the data subject an opportunity of responding by either consenting to the access or by providing reasons why the access should be denied. In the event that the data subject furnishes reasons for the support or denial of access, the Deputy Information Officer will consider these reasons in determining whether access should be granted to the requestor or not. The Deputy Information Officer has been delegated with the task of receiving and co-ordinating all requests for access to records in terms of PAIA, in order to ensure proper compliance with PAIA and POPIA. Should the Deputy Information Officer be unclear with regard to fulfilling and\or responding to any such request, same will be referred to the Information Officer, and if still unable to adequately address the query, the Information Officer will liaise with the appointed legal practitioners on all of these requests.

All requests in terms of PAIA and this Manual must be addressed to the Deputy Information Officer using the details in Section A above.

Records automatically available - [section 51(1) (c)]

At this stage no notice(s) has/have been published in terms of section 52 of the PAIA on the categories of records that are automatically available without a person having to request access in terms of the PAIA. Records that are automatically available at the registered offices of Zak Steel on payment of the prescribed fee for reproduction are:

1. Records of Zak Steel lodged in terms of government requirements such as the Registrar of Deeds;

2. Documentation and information relating to Zak Steel which is held by the Companies and Intellectual Properties Commission in accordance with the requirements set out in set out in section 25 of the Companies Act 71 of 2008;
3. Product and Services Brochures; and
4. News and other Marketing Information.
5. Certain other information relating to Zak Steel as is made available on their website from time to time.

INFORMATION AVAILABLE IN TERMS OF POPIA

In terms of POPIA, personal information must be processed for a specified purpose. The purpose for which data is processed by Zak Steel will depend on the nature of the data and the particular data subject. The purpose is ordinarily disclosed, explicitly or implicitly, at the time the data is collected.

SECTION D - CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION COLLECTED BY ZAK STEEL AND ITS ASSOCIATED ENTITIES

The list(s) below depict records of information which Zak Steel may have / has available in terms of laws applicable to it. Some of this information and the access thereto may be restricted to protect the Privacy and Private information of Data Subjects:

STATUTORY EMPLOYEE RECORDS

1. Employees' names, contact details and occupations;
2. Identity number and identity documents including passports;
3. Employment history and references;
4. Employee number;
5. Banking and financial details;
6. Details of payments to third parties (allowable deductions from salaries);
7. Employment contracts;
8. Attendance register;
9. Employment Equity plans;
10. Medical aid records;
11. Pension fund records;
12. Collective agreements;
13. Arbitration awards;
14. Leave records;
15. Parental status;
16. Biometrics;
17. Records of strikes, lockouts and protest action;
18. Training records;
19. Staff records (after date of employment ceases);
20. Expense accounts;
21. Payroll Records;
22. Disability status;

23. Marital status;
24. Criminal records;
25. Medical records.

HUMAN RESOURCES

1. BEE Statistics;
2. Career Development Records;
3. Personnel Information;
4. Employment Equity Reports;
5. General Terms of Employment;
6. Letter of Employment;
7. Performance Management Records;
8. Training manuals (Learning and Development);
9. Training Agreements;
10. Policies and Procedures;
11. CV's, application details;
12. Disciplinary Code and Records;
13. Disciplinary Procedures, CCMA and court matters, Retrenchment and legal processes re employment matters;
14. Job profiles;
15. SETA Records;
16. Social Responsibility.

CLIENTS AND PROSPECTIVE CLIENTS

1. Postal and/or street address;
2. Title and name;
3. Identity number or passport number;
4. Contact numbers and/or email address;
5. Ethnic group
6. Age;
7. Gender;
8. Marital status;
9. Nationality;
10. Language;
11. Financial information;
12. Browsing habits and click patterns on Zak Steel's website.

VENDORS/ SUPPLIERS/ OTHER BUSINESSES

1. Name and contact details;
2. Identity and/or company information and directors' information;
3. Banking and financial information;
4. Information about products or services;

5. Other information not specified, reasonably required to be processed for business operations.

Records that are not automatically available

Records of the Company which are not automatically available must be requested in terms of the procedure set out in section 8 of this PAIA Manual or the Regulations as set out in terms of POPIA, and which may be subject to the restrictions and right of refusal to access as provided for in the PAIA and in POPIA.

No request shall be accepted telephonically, nor shall any information be supplied telephonically. Only the Information officer or any Deputy Information officer appointed shall have the mandate to disclose information in terms of this manual.

CATEGORIES OF RECORDS AVAILABLE UPON REQUEST

Zak Steel maintains records on the categories and subject matters listed below. please note that the recordal of a category or subject matter in this Manual does not imply that a request for access to such records would be honoured. All requests for access will be evaluated on an ad hoc basis in accordance with the provisions of PAIA and POPIA.

Please note further that any records held by Zak Steel are those of third parties (such as clients and employees). Requests for access to these records will be considered very carefully. Please ensure that requests for such records are carefully motivated.

CATEGORY	RECORDS
1. Corporate internal records The records listed pertain Zak Steel's own affairs	1. Memorandum of Incorporation and\or Memoranda and Articles of Association 2. Operational records 3. Intellectual Property 4. Advertising records 5. Financial records 6. Service records 7. Legislation and statutory records 8. Internal communications 9. Resolutions and minutes of meetings 10. Internal procedures and regulations 11. All and any additional records constituting records relating to the affairs Zak Steel.
2. Employee records For the purposes of this section, "employee" refers to any person who works for or offers services to or on	1. Any personal records provided to Zak Steel by its employees. 2. Any records a third party has provided Zak Steel regarding their employees.

behalf of Zak Steel and accepts or is entitled to accept any compensation and any other person who supports or contributes in carrying out or conducting the business of Zak Steel. This includes directors, all employees (temporary, permanent, and part-time) staff as well as contract employees. The same applies to “employees”.	3. Employment policies and procedures. 4. Contractual and quasi-contractual employee agreements; 5. Internal evaluation and disciplinary records. 6. Other internal records and correspondence.
3. **<u>Client-related records</u>** For the purposes of this section “client” shall mean an existing client of Zak Steel as well as former clients and prospective clients and as may consist of individuals and\or legal entities.	1. Agreements concluded between Zak Steel and the client and/or other persons. 2. Recordings of the telephone conversations between employees of Zak Steel and Zak Steel’s client and third-party’s consumers if applicable. 3. Information received by Zak Steel from clients and as may be required to perform the contractual obligations Zak Steel is required to perform on behalf of any such client and\or third-party consumer.
4. **<u>Third-party records</u>** Records are kept in respect of other parties to which Zak Steel is a party, including agreements concluded with contractors and sub-contractors, suppliers, service providers, and providers of information regarding *inter alia* general market conditions and aspects of a similar nature. In addition, such other parties may possess records which are the property of or belong to Zak Steel.	1. Employee, client, or Zak Steel records which are held by another party as opposed to being held by Zak Steel in compliance with an agreement concluded by Zak Steel and the 3rd party, or in pursuant of Zak Steel’s business. 2. Records held by Zak Steel pertaining to other parties, including financial records, correspondence, contractual records, records provided by the other party, and records third parties have provided about the contractors or suppliers.
5. **<u>Ancillary records</u>**	1. Information that relates to or involves Zak Steel and is of a confidential and\or private nature. 2. Information obtained by Zak Steel after receipt of consent from a data subject and as is required to perform security objectives and fulfil insurance requirements. 3. Information obtained by Zak Steel in the course of conducting its business and

	fulfilling its corporate and commercial responsibilities.

Procedure for requesting access to the above information

Any request for access to a record in terms of PAIA must materially correspond and comply with Form C of Annexure B to Government Notice No. R187 dated 15 February 2002 (See Annexure "A" below). It should be noted that a request for access to information can be refused if the application does not comply with the requirement of the Act. The denied request will be returned to the requestor.

POPIA states that a data subject may (upon the provision of proof of identity) request Zak Steel to confirm (free of charge) all the information it holds about the data subject and may request access to such information, including information about the identity of third parties who have or have had access to such information ("Personal Requester").

A request will not automatically be granted and short reasons for the refusal shall be supplied. Further the completion and submission of a request does not automatically allow the requester access to the requested record.

The requester must comply with all the procedural requirements contained in the PAIA and POPI Acts relating to the request for access to records.

If any party wishes to request access to any of the above categories of information (Section C) such party is required to complete a request form as set out in Annexure "A" hereto. These forms are available from:

1. Our Information Officer (whose contact details are in Section A of this manual);
2. The SAHRC website (www.sahrc.org.za) and\or the Information Regulator (https://justice.gov.za/inforeg/)
3. The Department of Justice and Constitutional Development website (www.doj.gov.za).

A requester must state that the information is required in order to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. The requester must also provide an explanation of why the requested record is required for the exercise or protection of that right.

If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the information officer. The information officer will assist the applicable individual in completing the prescribed form and explain the detail to the applicable individual, thereafter the applicable individual will confirm the content of the prescribed form by attaching their mark or signature.

There is a prescribed fee (payable in advance) for requesting and accessing information in terms of the Act. Details of these fees are contained in the request form.

When a request is received by the information officer of the Company, the information officer shall by notice require the requester, other than a personal requester (referred to above), to pay the prescribed request fee, before further processing of the request.

A requester may also be called upon to pay the additional fees prescribed by regulation for searching for and compiling the information which he\she may have requested, including copying charges 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 the requested form.

The information officer shall withhold a record until the requester has paid the fee or fees as indicated. If a deposit has been paid in respect of a request for access, which is refused, then the information officer shall repay the deposit to the requester.

It is important to note that the successful completion and submission of an access request form does not automatically allow the requester access to the requested record. An application for access to a record is subject to certain limitations if the requested record falls within a certain category as specified within Chapter 3 Part B of the POPI Act.

Zak Steel will process the request within 30 days of receipt of the request and decide whether to grant or decline the request and give notice with reason (if required) to that effect.

The 30-day period within which Zak Steel has to decide whether to grant or refuse the request, may be extended for a further period of not more than 30 days, if the request is for a large volume of information, or the request requires a search for information held in another office and the information cannot reasonably be obtained within the original 30-day period. Zak Steel will notify the requester in writing should extension be sought.

If it is reasonably suspected that the requester has obtained access to records through the submission of materially false or misleading information, legal proceedings may be instituted against such requester.

The completed Access Request Form together with a copy of the identity document must be submitted via conventional mail or e-mail and must be addressed to the contact person as indicated above.

<u>Grounds for Refusal of Access to Records</u>

Zak Steel has the right to refuse access to information on legal grounds as set out in POPIA and\or in PAIA which will mainly be on one or more of the following grounds:

1. ***Mandatory protection of the personal information, special personal information or privacy of a third party who is a natural person (including children),*** if such disclosure would involve the unlawful or unreasonable disclosure of Personal Information about a third party,

including a deceased individual or child, subject to the provisions of section 63 (2) of PAIA or any section or regulation of POPIA.

2. ***Mandatory protection of the personal, confidential or commercial information of the third party (which may be a natural person or legal entity),*** if the record contains:
    2.1. Trade secrets of that party;
    2.2. Financial, commercial, scientific or technical information which disclosure could likely cause harm to the financial or commercial interest of that party;
    2.3. Information disclosed in confidence by the third party to Zak Steel if the disclosure could put the third party to a disadvantage in negotiations or commercial completion.
    2.4. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement;
3. ***Mandatory protection of certain confidential information of third party,*** where the head of a private body must refuse a request for access to a record of the body if its disclosure would constitute an action for breach of a duty of confidence owed to a third party in terms of an agreement.
4. ***Mandatory protection of the safety of individuals and the protection of property,*** where such disclosure could endanger the life or physical safety of an individual, or prejudice or impair the security of:
    4.1. a building, structure or any system
    4.2. a means of transport, or
    4.3. any other property.
5. ***Mandatory protection of records which could be regarded as privileged in legal proceedings,*** **unless** the legal privilege has been waived;
6. ***Mandatory protection of records and information as laid out in the National Key Point Act;***
7. ***Commercial information of private body,*** in that a request for access to a record may be refused if the record contains:
    7.1. trade secrets, financial, commercial, scientific or technical information of the institution, which disclosure, could likely cause harm to the financial or commercial interest of the institution;
    7.2. Information which, if disclosed could prejudice or put the institution at a disadvantage in negotiations or commercial competition; and
    7.3. A computer program which is owned by the institution, and which is protected by copyright.
8. ***Mandatory protection of research information of the institution.*** A request will be refused if this disclosure would disclose the identity of the institution, the researcher or the subject matter of the research and would place the researcher at a serious disadvantage.
9. ***Mandatory disclosure in public interest.*** Despite any of the protections mentioned above, the director of the Company shall grant a request for access to a record if:
    9.1. the disclosure of the record would reveal evidence of-
        1 a substantial contravention of, or failure to comply with, the law; or
        2 imminent and serious public safety or environmental risk; and
        3 the public interest in the disclosure of the record clearly outweighs the harm contemplated in the provision in question.

9.2. If disclosure of the record would prejudice or impair the security of property or means of transport;

9.3. If disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;

9.4. Disclosure of the record would put the Company at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;

9.5. The record is a computer programme, and the record contains information about research being carried out or about to be carried out on behalf of a third party or the Company.

<u>Remedies Available if Request for Information is refused</u>

If the request for access is refused, the Deputy Information Officer of the Company must:

1. State adequate reasons for the refusal, including the provisions of this Act relied on;
2. Exclude, from any such reasons, any reference to the content of the record; and
3. State that the requester may lodge an application with a court against the refusal of the request, and the procedure (including the period) for lodging the application.

<u>Internal Remedies</u>

Zak Steel does not have an internal appeal procedure. As such, the decision made by the Information Officer and the Deputy Information Officer pertaining to a request is final, and requestors will have to exercise such external remedies at their disposal if a request is refused, and the requestor is not satisfied with the response provided by the information officer.

<u>External Remedies</u>

A requestor that is dissatisfied with the information officer's refusal to disclose information, may within 30 days of notification of the decision, apply to a court for appropriate relief. For purposes of the PAIA and POPI Acts, courts that have jurisdiction over these applications are the Constitutional Court, the High Court or another court of similar status. The court will review the request and decide whether in fact the Deputy Information Officer of the Company should give the requester the information requested or not. A court hearing an application in terms of the PAIA and\ or POPI Act may grant any order that is just and equitable including orders:

1. Confirming, amending or setting aside the decision which is the subject of the application;
2. Requiring the Deputy Information Officer of the Company or relevant authority of a public body or the head of a private body to take such action or to refrain from taking such action, as the court considers necessary within the period mentioned in the court order;
3. Granting an interdict, interim or specific relief, a declaratory order or compensation; or
4. Granting an order as to costs.

<u>Records that cannot be found or do not exist</u>

If Zak Steel has searched for a record and it is believed that the record does not exist or cannot be found, the requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

If after notice is given, the record in question is found, the requester must be given access thereto unless the ground for the refusal of access exists.

If the request is declined for any reason the notice must include adequate reasons for the decision, together with the relevant provisions of the PAIA relied upon and provide the procedure to be followed should the requester wish appeal the decision.

Section 59 (POPI Act) provides that the Information Officer of the Company may serve a record and grant access only to that portion which the law does not prohibit access to.

Fees

The Act provides for two types of fees, namely:

1. A request fee, which will be a standard fee; and
2. An access fee, which must be calculated by considering reproduction costs, search and preparation time and costs, as well as postal costs.

When the request is received by the Deputy Information Officer of the Company, such person shall by notice require the requester to pay the prescribed request fee, if any, before further processing of the request.

If a requester requires access to records of his/her Personal Information, there shall be no request fee payable. However, the requester must pay the prescribed access and reproduction fees for such Personal Information.

If the search for the record has been made and the preparation of the record for disclosure including arrangements to make it available in the request form, requires more than the hours prescribed in the regulations for this purpose, the Deputy Information Officer of the Company shall notify the requester to pay as a deposit the prescribed portion of the access fee which would be payable if the request is granted.

The Deputy Information Officer of the Company shall withhold the record until the requester has paid the fees as indicated in Annexure “B” hereto.

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 records for disclosure including making arrangements to make it available in the request form.

If a deposit has been paid in respect of a request for access, which is refused, then the Deputy Information Officer of the Company must repay the deposit to the requester with interest at the prescribed rate.

<u>Third parties</u>

If the request is for the record pertaining to a third party, the Deputy Information Officer must take all reasonable steps to inform the third party of the request. This must be done within 21 (twenty-one) days of receipt of the request. The manner in which this is done must be by the fastest means reasonably possible, but if orally, the Deputy Information Officer of the Company must thereafter give the third party a written confirmation of the notification.

The third party may within 21 (twenty-one) days thereafter either make representation to Zak Steel as to why the request should be refused; alternatively grant written consent to the disclosure of the record.

The third party must be advised of the decision taken by the Deputy Information Officer of Zak Steel whether to grant or to decline the request. A third party who is dissatisfied with the Deputy Information Officer of the Company's decision to grant a request for information, may within 30 (thirty) days of notification of the decision, apply to a Court for relief.

SECTION E – INFORMATION AVAILABLE IN TERMS OF OTHER LEGISLATION [SECTION 51(1) (D)]

Where applicable to our operations, records are kept in accordance with the legislation outlined hereinbelow:

1. Administration of Estates Act 66 of 1965
2. Basic Conditions of Employment Act 75 of 1997
3. Broad-Based Black Economic Empowerment Act 53 of 2003
4. Close Corporations Act 69 of 1984
5. Companies Act 71 of 2008
6. Compensation for Occupational Injuries and Health Diseases Act 130 of 1993
7. Competition Act 89 of 1998
8. Consumer Protection Act 68 of 2008
9. Copyright Act 98 of 1978
10. Customs and Excise Act 91 of 1964
11. Customs Duty Act 30 of 2014
12. Debt Collectors Act 114 of 1998
13. Electronic Communications and Transactions Act 25 of 2002
14. Electronic Communications Act, 36 of 2005
15. Employment Equity Act 55 of 1998
16. Financial Advisory and Intermediary Services Act 37 of 2002
17. Financial Intelligence Centre Act 38 of 2001
18. Income Tax Act 58 of 1962

19. Insolvency Act No. 24 of 1936
20. Labour Relations Act 66 of 1995
21. Merchandise Marks Act 17 of 1941
22. National Credit Act 34 of 2005
23. Occupational Health & Safety Act 85 of 1993
24. Pension Funds Act 24 of 1956
25. Prevention of Organised Crime Act 121 of 1998
26. Prevention and Combating of Corrupt Activities Act 12 of 2004
27. Protection of Personal Information Act 4 of 2013;
28. Promotion of Access to Information Act 2 of 2000;
29. Promotion of Equality and Prevention of Unfair Discrimination ACT 4 OF 2000;
30. Protected Disclosures Act 26 Of 2000;
31. Skills Development Act 97 of 1998
32. Skills Development Levies Act 9 of 1999
33. Stamp Duties Act 77 of 1968
34. Stock Exchanges Control Act 1 of 1985 (and the rules and listing requirements of the JSE Securities Exchange authorised in terms thereof)
35. Unemployment Contributions Act 4 of 2002
36. Unemployment Insurance Act 30 of 1966
37. Value Added Tax Act 89 of 1991
38. Such other legislation as may from time to time be applicable.

While Zak Steel has used its best endeavours to supply you with a list of applicable legislation it is possible that the above list may be incomplete. Whenever it comes to Zak Steel's attention that existing or new legislation allows a requester access on a basis other than that set out in the PAIA or POPIA Acts, we shall update the list accordingly.

<u>Particulars in terms of section 51 of the PAIA</u>

On 9 March 2001 the PAIA came into effect. The PAIA seeks to advance a culture of transparency and accountability in both public and private bodies. The legislation was enacted as a direct response to Section 32(2) of the Constitution of South Africa – the right of access to information – which requires that the Government implements laws in an effort to make information pertaining to public and private bodies more accessible to all.

The Act gives 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. Where a request is made in terms of the PAIA, the body to whom the request is made is obliged to release the information, except where the PAIA expressly provides that the information may or must not be released.

One of the main requirements specified in the PAIA is the compilation of a manual that provides information on both the types and categories of records held by the public or private body. In terms of the PAIA, the Company is regarded as a "private body" and therefore the requirements regarding access must be in compliance with the provisions of the PAIA relevant to private bodies and more in particular Section 51 of the PAIA.

In compliance with Section 51 of the PAIA this PAIA Manual sets out the following details:

1. The Company's contact details including, physical and postal addresses, telephone and fax numbers, electronic mail address of the person tasked in terms of this Code of Conduct;
2. Information on how to obtain and access this Code of Conduct and a guide on how to use it;
3. Categories of information held by the Company that is available without a person having to formally request such details in terms of the PAIA;
4. Categories of information held by the Company that is available in accordance with other legislation and which, subject to the PAIA, may be made available by the Company on receipt of and consideration of a formal request, made in terms of the PAIA;
5. Sufficient information to facilitate a request for access to records and a description of the subjects on which records are available from the Company;
6. Adherence to these requirements entails not only compilation of the external manual but also compliance with the general provisions stated in the PAIA.

SECTION F – PROCESSING OF PERSONAL INFORMATION

1. BACKGROUND TO THE PROMOTION OF ACCESS TO INFORMATION ACT

This manual on data protection explains what information Zak Steel collects the information and how the collected information is used. For example, every piece of data that you provide via our website will be encrypted using Secure Sockets Layer (SSL) technology to prevent unauthorized access to a collection of such data.

We place great importance on the security of all personal data associated with our users. We have security measures in place to protect against the loss, misuse and alteration of personal information under our control.

Our security and privacy policies are periodically reviewed and adjusted as necessary and only authorized personnel has access to personal information.

Parliament assented to POPIA on 19 November 2013. The commencement date of section 1, Part A of Chapter 5, section 112 and section 113 is 11 April 2014. The commencement date of the other sections is 1 July 2021.

POPIA or POPI was promulgated on 26 November 2013. The Protection of Personal Information Act (POPIA) is intended to promote the right to privacy in the Constitution, while at the same time protecting the flow of information and advancing the right of access to and protection of information.

The Protection of Personal Information Act (POPIA) involves three parties (who can be natural or juristic persons):

- The data subject: the person to whom the information relates.
- The responsible party: the person who determines why and how to process. For example, profit companies, non-profit companies, governments, state agencies and people. Called controllers in other jurisdictions
- The operator: a person who processes personal information on behalf of the responsible party. For example, an IT vendor. Called processors in other jurisdictions.

The Protection of Personal Information Act places various obligations on the responsible party, which is the body ultimately responsible for the lawful processing of personal information. Responsible parties should only use operators that can meet the requirements of lawful personal information processing prescribed by the Protection of Personal Information Act.

As set out above, responsible parties determine the purpose for processing information, what information is processed, for how long and how it is processed. Where an operator is involved, the responsible party will still determine the purpose for processing etc. but will outsource the processing of the information to the operator. The responsible party therefore still makes all decisions in relation to the information and the operator acts in accordance with these decisions and on the instructions from the responsible party.

The responsible party remains ultimately accountable for ensuring that POPIA is complied with by both itself and all operators providing services to the responsible party. The outsourcing or sub-contracting of any processing activities to operators does not absolve the responsible party from liability. If the operator contravenes POPIA, the responsible party will still be held liable by the Information Regulator.

As with many other relationships, a contractual agreement between a responsible party and operator will prove very useful and high highly recommended in order to definitively address and govern the roles of each party and the boundaries of the relationship.

The agreement between the responsible party and operator addresses, at the least, the following points:

1. That the operator only acts within the ambit of the agreement/mandate with the responsible party;
2. The purpose for processing of the information;
3. What information may be processed by the operator;
4. What the operator may or may not do with the information outside of the processing mandate;
5. A duty to protect the information received, not share it with third parties without consent, to keep the information received confidential and to otherwise act within the ambit of POPIA;
6. Limit the operator from appointing further operators without the responsible party's knowledge or consent; and
7. Liability for the operator.

As mentioned above, the responsible party will be held ultimately liable by the Information Regulator for a breach of POPIA by the operator. The Information Regulator will impose this liability on the responsible party where the breach occurred within the scope of the mandate agreement between the responsible party and the operator and will not be diverted to the operator where the breach is as a result of the operator's failure to uphold the principles of POPIA.

Therefore, the agreement between the responsible party and the operator is extremely important for the responsible party as this agreement can result in the responsible party holding the operator liable for any claims that the Information Regulator and/or data subjects (the people whose personal information is being processed) bring against the responsible party as a result of a breach of POPIA by the operator. A liability clause will allow the responsible party to bring a claim for any loss suffered by the responsible party as a result of the operator's negligence or breach of POPIA. Some relief for a responsible party in this regard is where an operator breaches POPIA where the operator has exceeded his/her mandate. In these circumstances, the operator is seen to be acting as a responsible party in regard to the personal information as the operator is determining the purposes and means of processing.

GENERAL DESCRIPTION OF INFORMATION SECURITY MEASURES

Zak Steel takes extensive information security measures to ensure the security, confidentiality, integrity and availability of the Personal Information under its care. This is supported by appropriate technical and organisational measures designed to ensure that personal data remains confidential and secure against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Measures include:

1. Firewalls
2. Virus protection software and update protocols
3. Logical and physical access control;
4. Secure setup of hardware and software making up the IT infrastructure;

Outsourced Service Providers who process Personal Information on behalf of Zak Steel are contracted to implement security controls.

2. PURPOSE OF THE POPIA MANUAL

POPIA establishes the rights and duties that are designed to safeguard personal data. In terms of POPIA, the legitimate needs of organizations to collect and use personal data for business and other purposes are balanced against the right of individuals to have their right of privacy, in the form of their personal details, respected.

POPIA applies to a particular activity, i.e. the processing of personal data, rather than a particular person or organization. Therefore, if you process personal data then you must comply with POPIA and, in particular, you must handle personal data in accordance with POPIA' s data protection principles.

Therefore, if you collect or hold information about an identifiable individual or if you use, disclose, retain or destroy that information, you are likely to be processing personal data. The scope of POPIA is very wide and it applies to almost everything you might do with an individual's personal details including details of your employees.

3. CONTACT DETAILS OF THE DIRECTORS

Directors:	Kim Lee Wilson Michael-Jon van Loggerenberg
Registered Address:	4 Boniface Road Selection Park Industrial Sites Springs 1559
Email Address:	kim@clydeind.co.za mj@clydeind.co.za
Telephone Number:	+27 11 815 5043
Website:	www.zak.co.za

POPI designates the head of the business as the Information Officer. Depending on the type of business, the Information Officer will therefore be the sole trader, a partner in a partnership or CEO (or equivalent) in a company or CC.

The head of the business can delegate his or her responsibilities as Information Officer to any other duly authorised person. However, it is important to note that whoever "determines the purpose of and means for processing personal information" remains ultimately responsible for ensuring that the processing of personal information is done in a lawful manner and "retains the accountability and responsibility for any power or the functions authorised to that person"

The Guidance Note specifies that "Each subsidiary of a group of companies must register its Information Officer".

The Information Officer must appoint as many Deputy Information Officers as necessary. For example, the appointment of Deputy Information Officers may become necessary to make the organisations records as accessible as reasonably possible for requesters. This must be done in writing, specifically using Template "B" in the Guidance Note which also stipulates that the DIO "should report to the highest management office within a Body" and therefore must be an employee.

4. DUTIES AND RESPONSIBILITIES

Duties and responsibilities of the Information Officer? The specific duties are spelled out for us in the Guidance Note.

The Act stipulates the following general responsibilities:

1. to encourage compliance with POPI;
2. dealing with requests made to the organisation in relation to POPI (for instance, requests from Data Subjects to update or view their personal information);
3. working with the Regulator in relation to investigations;
4. otherwise ensuring compliance with POPI;
5. as may be prescribed (i.e. keep an eye on the Regulator's website!).

Information Officers need to be registered with the Regulator before taking up their duties.

Regulation 4 lists the following prescribed responsibilities in addition to those listed above:

Compliance framework:

1 Develop and implement a compliance framework;
2 ensure it is monitored and maintained over time.

5. THE INFORMATION OFFICER

On a day-to-day basis the Information Officer may find themselves:

1. making recommendations and raising concerns where appropriate;
2. documenting information processing procedures;
3. evaluating and further developing data protection and security policies;
4. suggesting, selecting and implementing technical security measures;
5. drafting forms and contracts appropriate for data protection;
6. selecting employees, service providers and others to be involved in the processing of personal information monitoring data privacy and security measures as well as the proper use of data processing programs;
7. handling complaints relating to personal information;
8. employee training; and
9. preparing, submitting and maintaining notifications to the Regulator.

6. CONTACT DETAILS OF THE INFORMATION OFFICER

Designated Information Officer:	Michael Van Loggerenberg
Physical Address:	4 Boniface Road Selection Park Industrial Sites Springs 1559
Email:	mj@clydeind.co.za

7. WHAT INFORMATION DO WE COLLECT?

Collection of Personal Information

We collect and process your Personal Information mainly to provide you with access to our services and products, to help us improve our offerings to you, to support our contractual relationship with our clients and you and for certain other purposes explained below. The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose. We collect information directly from you where you provide us with your personal details, for example when you purchase or supply a product or services to or from us or when you submit enquiries to us or contact us. We also collect information when such is supplied by the client's with whom we have contracts requiring the provision of such information and as is necessary for us to comply with our contractual obligations. Where possible, we will inform you what information you are required to provide to us and what information is optional.

Examples of information we collect from you are:

1. Name
2. Address
3. email address
4. Telephone/cell number
5. Identity Number/Passport Number

We collect and process your Personal Information mainly to provide you with access to our services, delivery of goods and products, to help us improve our offerings to you, to support our contractual relationship with our clients and you and for certain other purposes explained below. The type of information we collect will depend on the purpose for which it is collected and used. We will only collect information that we need for that purpose.

Collection of Non-Personal Information

<u>Website:</u>

We may automatically collect non-Personal Information about you such as the type of internet browsers you use or the website from which you linked to our website. We may also aggregate details which you have submitted to the site (for example, the products or services you are interested in). You cannot be identified from this information and it is only used to assist us in providing an effective service on our web site. We may, from time-to-time supply third parties with this non-personal or aggregated data for uses in connection with this website.

<u>Cookies policy</u>

The Internet pages of Zak Steel use cookies. Cookies are text files that are stored in a computer system via an Internet browser. Many Internet sites and servers use cookies. Many cookies contain a so-called cookie ID. A cookie ID is a unique identifier of the cookie. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the data subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

Through the use of cookies, we can provide the users of our website with more user-friendly services that would not be possible without the cookie setting. By means of a cookie, the information and offers on our website can be optimized with the user in mind. Cookies allow us, as previously mentioned, to recognize our website users. The purpose of this recognition is to make it easier for users to utilize our website. The website user that uses cookies, e.g. does not have to enter access data each time the website is accessed, because this is taken over by the website, and the cookie is thus stored on the user's computer system.

Another example is the cookie of a shopping cart in an online shop. The online store remembers the articles that a customer has placed in the virtual shopping cart via a cookie. The data subject may, at any time, prevent the setting of cookies through our website by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies. Furthermore, already set cookies may be deleted at any time via an Internet browser or other software programs. This is possible in all popular Internet browsers. If the data subject deactivates the setting of cookies in the Internet browser used, not all functions of our website may be entirely usable.

Registration on our website

The data subject has the possibility to register on the website of the Responsible Party with the indication of personal data. Which personal data is transmitted to the Responsible Party as determined by the respective input mask used for the registration. The personal data entered by the data subject is collected and stored exclusively for internal use by the Responsible Party, and for its own purposes. The Responsible Party may request transfer to one or more operators (e.g. a parcel service) that also uses personal data for an internal purpose which is attributable to the Responsible Party.

By registering on the website of the Responsible Party, the IP address - assigned by the Internet service provider (ISP) and used by the data subject - date, and time of the registration are also stored. The storage of this data takes place against the background that this is the only way to prevent the misuse of our services, and, if necessary, to make it possible to investigate committed offenses. Insofar, the storage of this data is necessary to secure the Responsible Party. This data is not passed on to third parties unless there is a statutory obligation to pass on the data, or if the transfer serves the aim of criminal prosecution.

The registration of the data subject, with the voluntary indication of implied consent that the personal data, is intended to enable the Responsible Party to offer the data subject contents or services that may only be offered to registered users due to the nature of the matter in question. Registered persons are free to change or withdraw their consent specified during the registration at any time, or to have them completely deleted from the data stock of the Responsible Party.

The data Responsible Party shall, at any time, provide information upon request to each data subject as to what personal data is stored about the data subject. In addition, the data Responsible Party shall correct or erase personal data at the request or indication of the data subject, insofar as there are no statutory storage obligations to keep the data. The entirety of the Responsible Party's employees is available to the data subject in this respect as contact persons.

Contractual Obligations

The data subject may conclude an agreement with a Zak Steel client with the indication of personal data. The personal data is transmitted to Zak Steel by the relevant client for the purpose of Zak Steel fulfilling its contractual obligations to the client. The personal data entered by the data subject or obtained by Zak Steel's client is collected and stored exclusively for internal use by the Responsible Party, and for its own purposes. The Responsible Party may request transfer to one or more operators (e.g. a parcel service) that also uses personal data for an internal purpose which is attributable to the Responsible Party.

The agreement as between Zak Steel's client and the data subject makes provision for the voluntary indication of implied consent that the personal data, is intended to enable the Responsible Party to offer the data subject contents or services that may only be offered to consumers due to the nature of the matter in question. The consumer is free to change or withdraw their consent specified during the registration with client at any time, or to have them completely deleted from the data stock of the Responsible Party.

The data Responsible Party shall, at any time, provide information upon request to each data subject as to what personal data is stored about the data subject. In addition, the data Responsible Party shall correct or erase personal data at the request or indication of the data subject, insofar as there are no statutory storage obligations to keep the data. The entirety of the Responsible Party's employees is available to the data subject in this respect as contact persons.

A further contractual obligation requires that we arrange for the collection and delivery of goods acquired by you from a Zak Steel's client in the event of the goods being incorrect, damaged or not operating correctly. Under these circumstances, you may contact our call centre for the purposes of arranging for the collection of such goods being returned. Under these circumstances, the data subject will consent verbally to provide all personal details to enable compliance with Zak Steel's contractual obligations to the client. The agreement as between Zak Steel's client and the data subject makes provision for the voluntary indication of implied consent that the personal data, is intended to enable Zak Steel to offer the data subject contents or services that may only be offered to consumers due to the nature of the matter in question. The consumer is free to change or withdraw their consent specified during the verbal discussions with Zak Steel at any time, or to have them completely deleted from the data stock of Zak Steel subject to Zak Steel's contractual obligations to its clients with regard to retention of such information.

8. HOW WE USE YOUR INFORMATION

We will use your Personal and Non-Personal Information only for the purposes for which it was collected or agreed with you, for example:

- To allow for the delivery or collection of goods, the Personal and Non-Personal Information will be transferred to a courier service designated for delivery or collection of goods;
- For audit and record keeping purposes;
- For monitoring and auditing usage;
- For security and control reasons;
- In connection with legal proceedings;
- To assist with business development;
- To carry out our obligations arising from any contracts entered into between you and us alternatively us and our clients with whom you may have contracted;
- To conduct market or customer satisfaction research or for statistical analysis;
- To confirm and verify your identity or to verify that you are an authorised customer for security purposes;
- To respond to your queries or comments.

We will also use your Personal Information to comply with legal and regulatory requirements or industry codes to which we subscribe or which apply to us, or when it is otherwise allowed by law;

9. INFORMATION RETENTION

Where we collect Personal Information for a specific purpose, we will not keep it for longer than is necessary to fulfil that purpose, unless we have to keep it for legitimate business or legal reasons.

In order to protect information from accidental or malicious destruction, when we delete information from our services we may not immediately delete residual copies from our servers or remove information from our backup systems;

10. DISCLOSURE OF PERSONAL INFORMATION

We may disclose your Personal Information to our business partners who are involved in the delivery of products or services to you. We have agreements in place to ensure that they comply with these privacy terms.

You consent to us disclosing your personal information obtained from you with:

1. third parties for the purposes listed above;
2. where we have a duty or a right to disclose in terms of law or industry codes;
3. where we believe it is necessary to protect our rights;
4. we are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorised access and use of personal information. we will, on an on-going basis, continue to review our security controls and related processes to ensure that your personal information is secure;
5. acceptable usage of personal information;
6. computer and network security;
7. governance and regulatory issues;
8. investigating and reacting to security incidents;
9. monitoring access and usage of personal information;
10. physical security;
11. retention and disposal of information;
12. secure communications;
13. security in contracting out activities or functions;
14. All and any other statutorily permissible purposes.

When we contract third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that Personal Information that we remain responsible for, is kept secure.

We will ensure that anyone to whom we pass your Personal Information agrees to treat your information with the same level of protection as we are obliged to.

11. ACCESS TO YOUR PERSONAL INFORMATION

You have the right to request a copy of the Personal Information we hold about you. To do this, simply contact us at the numbers/addresses listed above and specify what information you would like. Please note that a formally motivated request will be required to enable release of the information requested. We will take all reasonable steps to confirm your identity before providing details of your personal information.

Please note that any such access request may be subject to a payment of a legally allowable fee, as laid down in our PAIA Policy.

12. CORRECTION OF YOUR PERSONAL INFORMATION

You have the right to ask us to update, correct or delete your personal information. We will take all reasonable steps to confirm your identity before making changes to Personal Information we may hold about you. We would appreciate it if you would take the necessary steps to keep your Personal Information accurate and up-to-date by notifying us of any changes we need to be aware of.

13. RETENTION OF PERSONAL DATA

We will retain your data in compliance with the POPIA and in compliance with other applicable legislation.

Routine Erasure and Blocking of Personal Data
The data Responsible Party shall process and store the personal data of the data subject only for the period necessary to achieve the purpose of storage, or as far as this is granted by the POPIA or other legislators in laws or regulations to which the Responsible Party is subject to.

If the storage purpose is not applicable, or if a storage period prescribed by the POPIA or another competent legislator expires, the personal data will be destroyed.

14. **RIGHTS OF THE DATA SUBJECT**

A) **RIGHT OF CONFIRMATION**
Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party the confirmation as to whether or not personal data concerning him or her is being processed. If a data subject wishes to avail himself of this right of confirmation, he or she may, at any time, contact Designated Official.

B) **RIGHT OF ACCESS**

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party free of charge information about his or her personal data stored at any time and a copy of this information. Furthermore, the PAIA grants the data subject access to the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Responsible Party rectification or erasure of personal data, or restriction of processing of personal data concerning the data subject, or to object to such processing;
- the existence of the right to lodge a complaint with a supervisory authority;
- where the personal data is not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) of the PAIA and, at least in those cases, meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.

Furthermore, the data subject shall have a right to obtain information as to whether personal data is transferred to a third country or to an international organization. Where this is the case, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

If a data subject wishes to avail himself of this right of access, he or she may at any time contact our Designated Officer.

C) **RIGHT TO RECTIFICATION**

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party without undue delay the rectification of inaccurate personal data concerning him or her.

Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

If a data subject wishes to exercise this right to rectification, he or she may, at any time, contact our Information Officer for this purpose.

D) **RIGHT TO ERASURE (RIGHT TO BE FORGOTTEN)**

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party the erasure of personal data concerning him or her without undue delay, and the Responsible Party shall have the obligation to erase personal data without undue delay where one of the following grounds applies, as long as the processing is not necessary:

- The personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed.
- The data subject withdraws consent to which the processing is based according to point POPIA and where there is no other legal ground for the processing.
- The data subject objects to the processing pursuant to POPIA and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to POPIA.
- The personal data have been unlawfully processed.
- The personal data must be erased for compliance with a legal obligation in South Africa which the Responsible Party is subject.
- If one of the aforementioned reasons applies, and a data subject wishes to request the erasure of personal data stored by Zak Steel, he or she may at any time contact the Designated Officer. The Designated Officer shall promptly ensure that the erasure request is complied with immediately. Where the Responsible Party has made personal data public and is obliged pursuant to POPIA to erase the personal data, the Responsible Party, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other Responsible Party's processing the personal data that the data subject has requested erasure by such Responsible Party's of any links to, or copy or replication of, those personal data, as far as processing is not required. An employee of the business will arrange the necessary measures in individual cases.

E) **RIGHT OF RESTRICTION OF PROCESSING**

Each data subject shall have the right granted by the South African Regulator to obtain from the Responsible Party restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by the data subject, for a period enabling the Responsible Party to verify the accuracy of the personal data.
- The processing is unlawful and the data subject opposes the erasure of the personal data and requests instead the restriction of their use instead.

- The Responsible Party no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.
- The data subject has objected to processing pursuant to POPIA pending the verification whether the legitimate grounds of the Responsible Party override those of the data subject.

If one of the aforementioned conditions is met, and a data subject wishes to request the restriction of the processing of personal data stored by Zak Steel, he or she may at any time contact the Designated Officer. The Designated Officer will arrange the restriction of the processing.

F) **RIGHT TO OBJECT**

Each data subject shall have the right granted by the South African Regulator to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her, which is based on POPIA. This also applies to profiling based on these provisions. Under these circumstances:

- the business shall no longer process the personal data in the event of the objection unless it can demonstrate compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject, or for the establishment, exercise or defense of legal claims.
- If the business processes personal data for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing.
- This applies to profiling to the extent that it is related to such direct marketing. If the data subject objects to the business to the processing for direct marketing purposes, the business will no longer process the personal data for these purposes.
- In addition, the data subject has the right, on grounds relating to his or her particular situation, to object to processing of personal data concerning him or her by the business for scientific or historical research purposes, or for statistical purposes pursuant to POPIA, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

In order to exercise the right to object, the data subject may directly contact the Designated Officer.

G) **AUTOMATED INDIVIDUAL DECISION-MAKING, INCLUDING PROFILING**

Each data subject shall have the right granted by the South African Regulator not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her, or similarly significantly affects him or her, as long as the decision:

1. is not necessary for entering into, or the performance of, a contract between the data subject and a data Responsible Party, or
2. is not authorised by the national law to which the Responsible Party is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, or
3. is not based on the data subject's explicit consent.

If the decision:

1. is necessary for entering into, or the performance of, a contract between the data subject and a data Responsible Party, or
2. it is based on the data subject's explicit consent,

the business shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Responsible Party, to express his or her point of view and contest the decision.

If the data subject wishes to exercise the rights concerning automated individual decision-making, he or she may at any time directly contact our Information Regulator of the business another employee of the Responsible Party.

H) **RIGHT TO WITHDRAW DATA PROTECTION CONSENT**

Each data subject shall have the right granted by the South African Regulator the right to withdraw his or her consent to processing of his or her personal data at any time. If the data subject wishes to exercise the right to withdraw the consent, he or she may at any time directly contact the Designated Officer.

I) **LEGAL BASIS FOR THE PROCESSING**

POPIA serves as the legal basis for processing operations for which we obtain consent for a specific processing purpose. If the processing of personal data is necessary for the performance of a contract to which the data subject is party, as is the case, for example, when processing procedures are necessary for the supply of goods or to provide any other service, the processing is based on POPIA. The same applies to such processing operations which are necessary for carrying out pre-contractual measures, for example in the case of inquiries concerning our products or services. If Zak Steel is subject to a legal obligation by which processing of personal data is required, such as for the fulfilment of tax obligations, the processing is based on POPIA. In rare cases, the processing of personal data may be necessary to protect the vital interests of the data subject or of another natural person.

J) **ACTUAL OR PLANNED TRANS-BORDER FLOWS OF PERSONAL INFORMATION**

Personal Information may be transmitted trans-border to Zak Steel‘s authorised dealers and its suppliers in other countries, and Personal Information may be stored in data servers hosted outside South Africa, which may not have adequate data protection laws. Zak Steel will endeavour to ensure that its dealers and suppliers will make all reasonable efforts to secure said data and Personal Information.

K) **PERIOD FOR WHICH THE PERSONAL DATA WILL BE STORED**

The criteria used to determine the period of storage of personal data is the respective statutory retention period. After expiration of that period, the corresponding data is routinely deleted, as long as it is no longer necessary for the fulfilment of the contract or the initiation of a contract.

We clarify that the provision of personal data is partly required by law (e.g. tax regulations) or can also result from contractual provisions (e.g. information on the contractual partner). Sometimes it may be necessary to conclude a contract that the data subject provides us with personal data, which must subsequently be processed by us. The data subject is, for example, obliged to provide us with personal data when our company signs a contract with him or her. The non-provision of the personal data would have the consequence that the contract with the data subject could not be concluded. Before personal data is provided by the data subject, the data subject must contact our Data Protection Officer. An employee of the business clarifies to the data subject whether the provision of the personal data is required by law or contract or is necessary for the conclusion of the contract, whether there is an obligation to provide the personal data and the consequences of non-provision of the personal data. Retention schedule of respective legislation are indicated below.

L) **HARD COPIES**

Documents are stored in an archive at different locations.

Companies Act, No 71 of 2008.

With regard to the Companies Act, No 71 of 2008 and the Companies Amendment Act No 3 of 2011, hardcopies of the documents mentioned below must be retained for 7 years:

- Any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Act;
- Notice and minutes of all shareholders meeting, including resolutions adopted and documents made available to holders of securities;
- Copies of reports presented at the annual general meeting of the company;
- Copies of annual financial statements required by the Act;
- Copies of accounting records as required by the Act;
- Record of directors and past directors, after the director has retired from the company;
- Written communication to holders of securities; and
- Minutes and resolutions of directors' meetings, audit committee and directors' committees;
- Copies of the documents mentioned below must be retained indefinitely:
- Registration certificate ;
- Memorandum of Incorporation and alterations and amendments;
- Rules;
- Securities register and uncertified securities register;
- Register of company secretary and auditors; and
- Regulated companies (companies to which chapter 5, part B, C and Takeover Regulations apply) – Register of disclosure of person who holds beneficial interest equal to or in excess of 5% of the securities of that class issued.

Consumer Protection Act, No 68 of 2008

The Consumer Protection Act seeks to promote a fair, accessible and sustainable market-place and therefore requires a retention period of 3 years for information provided to a consumer by an intermediary such as:

- Full names, physical address, postal address and contact details;
- ID number and registration number;
- Contact details of public officer in case of a juristic person;
- Service rendered;
- Intermediary fee;

- Cost to be recovered from the consumer;
- Frequency of accounting to the consumer;
- Amounts, sums, values, charges, fees, remuneration specified in monetary terms;
- Disclosure in writing of a conflict of interest by the intermediary in relevance to goods or service to be provided;
- Record of advice furnished to the consumer reflecting the basis on which the advice was given;
- Written instruction sent by the intermediary to the consumer ;
- Conducting a promotional competition refer to Section 36(11)(b) and Regulation 11 of Promotional Competitions;
- Documents Section 45 and Regulation 31 for Auctions.

<u>National Credit Act, No 34 of 2005</u>

The National Credit Act aims to promote a fair and transparent credit industry which requires the retention of certain documents for a specified period.
Retention for 3 years from the earliest of the dates of which the registrant created, signed or received the document or from the date of termination of the agreement or in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application which applies to the documents mentioned below:
<u>Regulation 55(1)(b):</u>

- Records of registered activities such as an application for credit declined;
- Reason for the decline of the application for credit;
- Pre-agreement statements and quotes;
- Documentation in support of steps taken in terms of section 81(2) of the Act;
- Record of payments made;
- Documentation in support of steps taken after default by consumer.

<u>Regulation 55(1)(c) in respect of operations:</u>

- Record of income, expenses and cash flow;
- Credit transaction flows;
- Management accounts and financial statements.

<u>Regulation 55(1)(d) with regard to the Credit Bureau:</u>

- All documents relating to disputes, inclusive of but not limited to, documents from the consumer;
- Documents from the entity responsible for disputed information;
- Documents pertaining to the investigation of the dispute;
- Correspondence addressed to and received from sources of information as set out in section 70(2) of the Act and Regulation 18(7) pertaining to the issues of the disputed information.

<u>Regulation 55(1)(a) with regard to Debt Counsellors:</u>

- Application for debt review;
- Copies of all documents submitted by the consumer;
- Copy of rejection letter;
- Debt restructuring proposal;
- Copy of any order made by the tribunal and/or the court and a copy of the clearance certificate.

<u>Regulation 56 with regard to section 170 of the Act:</u>

- Application for credit;
- Credit agreement entered into with the consumer.
- Regulation 17(1) with regard to Credit Bureau information:

Documents with a required retention period of the earlier of 10 years or a rehabilitation order being granted:

- Sequestrations
- Administration orders.

Documents with a required retention period of 5 years:

- Rehabilitation orders
- Payment profile.

Documents with a required retention period of the earlier of 5 years or until judgment is rescinded by a court or abandoned by the credit provider in terms of section 86 of the Magistrate's Court Act No 32 of 1944:

- Civil Court Judgments/Enquiries.

Documents with a required retention period of 1.5 years:

- Details and results of disputes lodged by the consumers.
- Documents with a required retention period of 1 year:
- Adverse information.

Documents with an unlimited required retention period:

- Liquidation.

Documents required to be retained until a clearance certificate is issued:

- Debt restructuring.
- Financial Advisory and Intermediary Services Act, No 37 of 2002:

Section 18 of the Act requires a retention period of 5 years, except to the extent that it is exempted by the registrar for the below mentioned documents:

- Known premature cancellations of transactions or financial products of the provider by clients;
- Complaints received together with an indication whether or not any such complaint has been resolved;
- The continued compliance with this Act and the reasons for such non-compliance;
- And the continued compliance by representatives with the requirements referred to in section 13(1) and (2).

The General Code of Conduct for Authorized Financial Services Provider and Representatives requires a retention period of 5 years for the below mentioned documents:

- Proper procedures to record verbal and written communications relating to a financial service rendered to a client as are contemplated in the Act, this Code or any other Code drafted in terms of section 15 of the Act;
- Store and retrieve such records and any other material documentation relating to the client or financial services rendered to the client;

And keep such client records and documentation safe from destruction;

All such records must be kept for a period after termination to the knowledge of the provider of the product concerned or in any other case after the rendering of the financial service concerned.

Financial Intelligence Centre Act, No 38 of 2001:

Section 22 and 23 of the Act require a retention period of 5 years for the documents and records of the activities mentioned below:

- Whenever an accountable transaction is concluded with a client, the institution must keep record of the identity of the client;

- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the clients' authority to act on behalf of that other person;
- If another person is acting on behalf of the client, the identity of that person and that other person's authority to act on behalf of the client;
- The manner in which the identity of the persons referred to above was established;
- The nature of that business relationship or transaction;
- In the case of a transaction, the amount involved and the parties to that transaction;
- All accounts that are involved in the transactions concluded by that accountable institution in the course of that business relationship and that single transaction;
- The name of the person who obtained the identity of the person transacting on behalf of the accountable institution;
- Any document or copy of a document obtained by the accountable institution. These documents may also be kept in electronic format.

<u>Compensation for Occupational Injuries and Diseases Act, No 130 of 1993:</u>

<u>Section 81(1) and (2)</u> of the Compensation for Occupational Injuries and Diseases Act requires a retention period of 4 years for the documents mentioned below:

- Register, record or reproduction of the earnings, time worked, payment for piece work and overtime and other prescribed particulars of all the employees.

<u>Section 20(2)</u> documents with a required retention period of 3 years:

- Health and safety committee recommendations made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation;
- Records of incidents reported at work.
- Asbestos Regulations, 2001, regulation 16(1) requires a retention period of minimum 40 years for the documents mentioned below:
- Records of assessment and air monitoring, and the asbestos inventory;
- Medical surveillance records;
- Hazardous Biological Agents Regulations, 2001, Regulations 9(1) and (2):
- Records of risk assessments and air monitoring;
- Medical surveillance records.

<u>Lead Regulations, 2001, Regulation 10:</u>

- Records of assessments and air monitoring;
- Medical surveillance records.

<u>Noise - induced Hearing Loss Regulations, 2003, Regulation 11:</u>

- All records of assessment and noise monitoring;
- All medical surveillance records, including the baseline audiogram of every employee.

<u>Hazardous Chemical Substance Regulations, 1995</u>, Regulation 9 requires a retention period of 30 years for the documents mentioned below:

- Records of assessments and air monitoring;
- Medical surveillance records.

<u>Basic Conditions of Employment Act, No 75 of 1997:</u>

The Basic Conditions of Employment Act requires a retention period of 3 years for the documents mentioned below:

<u>Section 29(4):</u>

- Written particulars of an employee after termination of employment;

<u>Section 31:</u>

- Employee's name and occupation;

- Time worked by each employee;
- Remuneration paid to each employee;
- Date of birth of any employee under the age of 18 years.

Employment Equity Act, No 55 of 1998:

Section 26 and the General Administrative Regulations, 2009, Regulation 3(2) requires a retention period of 3 years for the documents mentioned below:

- Records in respect of the company's workforce, employment equity plan and other records relevant to compliance with the Act;

Section 21 and Regulations 4(10) and (11) require a retention period of 3 years for the report which is sent to the Director General as indicated in the Act.

Labour Relations Act, No 66 of 1995:

Sections 53(4), 98(4) and 99 require a retention period of 3 years for the documents mentioned below:

- The Bargaining Council must retain books of account, supporting vouchers, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and registered employer's organizations must retain books of account, supporting vouchers, records of subscriptions or levies paid by its members, income and expenditure statements, balance sheets, auditor's reports and minutes of the meetings;
- Registered Trade Unions and employer's organizations must retain the ballot papers;
- Records to be retained by the employer are the collective agreements and arbitration awards.

Sections 99, 205(3), Schedule 8 of Section 5 and Schedule 3 of Section 8(a) require an indefinite retention period for the documents mentioned below:

- Registered Trade Unions and registered employer's organizations must retain a list of its members;
- An employer must retain prescribed details of any strike, lock-out or protest action involving its employees;
- Records of each employee specifying the nature of any disciplinary transgressions, the actions taken by the employer and the reasons for the actions;
- The Commission must retain books of accounts, records of income and expenditure, assets and liabilities.

Unemployment Insurance Act, No 63 of 2002:

The Unemployment Insurance Act, applies to all employees and employers except:

- Workers working less than 24 hours per month;
- Learners;
- Public servants;
- Foreigners working on a contract basis;
- Workers who get a monthly State (old age) pension;
- Workers who only earn commission.

Section 56(2)(c) requires a retention period of 5 years, from the date of submission, for the documents mentioned below:

- Employers must retain personal records of each of their current employees in terms of their names, identification number, monthly remuneration and address where the employee is employed.

Tax Administration Act, No 28 of 2011:

Section 29 of the Tax Administration Act, states that records of documents must be retained to:

- Enable a person to observe the requirements of the Act;
- Are specifically required under a Tax Act by the Commissioner by the public notice;
- Will enable SARS to be satisfied that the person has observed these requirements.

Section 29(3)(a) requires a retention period of 5 years, from the date of submission for taxpayers that have submitted a return and an indefinite retention period, until the return is submitted, then a 5 year period applies for taxpayers who were meant to submit a return, but have not

Section 29(3)(b) requires a retention period of 5 years from the end of the relevant tax period for taxpayers who were not required to submit a return, but had capital gains/losses or engaged in any other activity that is subject to tax or would be subject to tax but for the application of a threshold or exemption.

Section 32(a) and (b) require a retention period of 5 years but records must be retained until the audit is concluded or the assessment or decision becomes final, for documents indicating that a person has been notified or is aware that the records are subject to an audit or investigation and the person who has lodged an objection or appeal against an assessment or decision under the TAA.

Income Tax Act, No 58 of 1962:

Schedule 4, paragraph 14(1)(a)-(d) of the Income Tax Act requires a retention period of 5 years from the date of submission for documents pertaining to each employee that the employer shall keep:

- Amount of remuneration paid or due by him to the employee;
- The amount of employees tax deducted or withheld from the remuneration paid or due;
- The income tax reference number of that employee;
- Any further prescribed information;
- Employer Reconciliation return.

Schedule 6, paragraph 14(a)-(d) requires a retention period of 5 years from the date of submission or 5 years from the end of the relevant tax year, depending on the type of transaction for documents pertaining to:

- Amounts received by that registered micro business during a year of assessment;
- Dividends declared by that registered micro business during a year of assessment;
- Each asset as at the end of a year of assessment with cost price of more than R10 000;
- Each liability as at the end of a year of assessment that exceeded R 10 000.

Value Added Tax Act, No 89 of 1991:

Section 15(9), 16(2) and 55(1)(a) of the Value Added Tax Act and Interpretation Note 31, 30 March requires a retention period of 5 years from the date of submission of the return for the documents mentioned below:

- Where a vendor’s basis of accounting is changed the vendor shall prepare lists of debtors and creditors showing the amounts owing to the creditors at the end of the tax period immediately preceding the changeover period;

- Importation of goods, bill of entry, other documents prescribed by the Custom and Excise Act and proof that the VAT charge has been paid to SARS;
- Vendors are obliged to retain records of all goods and services, rate of tax applicable to the supply, list of suppliers or agents, invoices and tax invoices, credit and debit notes, bank statements, deposit slips, stock lists and paid cheques;
- Documentary proof substantiating the zero rating of supplies;
- Where a tax invoice, credit or debit note, has been issued in relation to a supply by an agent or a bill of entry as described in the Customs and Excise Act, the agent shall maintain sufficient records to enable the name, address and VAT registration number of the principal to be ascertained.

M) **ELECTRONIC STORAGE**

- The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with IT who will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.
- Scanned documents:
  - If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, with the exception of documents pertaining to personnel. Any document containing information on the written particulars of an employee, including: employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.
- Section 51 of the Electronic Communications Act No 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.

It is also required that all personal information which has become obsolete must be destroyed.

N) **DESTRUCTION OF DOCUMENTS**

Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and also to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

After completion of the process the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Registration. The documents are then made available for collection by the removers of the Company's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information. Documents may also be stored off-site, in storage facilities approved by the Company.

Contact details of the administrator responsible for this policy shall mean the details of the Information Officer outlined above.

14. COMPLAINTS PROCEDURE

You may also lodge a complaint with the Regulator in terms of section 63(3) if you are unhappy about the determination of an adjudicator as appointed by the Regulator, after the Regulator has investigated your complaint, by using form 5. The determination will have effect, until such time that the Regulator changes or overrules the determination post your complaint.

The complaint to the Regulator must be made in writing and should you experience any problems, you may contact the office of the Regulator who will provide you with reasonable assistance to make the complaint in writing.

The Regulator has the following powers when a complaint is lodged:

1. Consult with the RESPONSIBLE PARTY and with the complainant;
2. Investigate the complaint by gathering information through subpoenas and warrants or search premises;
3. Summons people to appear and testify or compel them to provide written evidence;
4. Conduct private interviews with people;
5. Conduct any enquiry she sees fit; and
6. Resolve the complaint by means of dispute resolution such as mediation and conciliation;
7. Apply for fines and penalties to be ordered by a competent court as set out in section 107 and 109 of POPIA;
8. Refer the matter to an enforcement committee and issue enforcement notices or information notices;
9. Institute civil action for damages.

SOURCES

- SAICA Guidelines-Updated October 2013 (also refers to the Banks Act and Insolvency Act);
- Companies Act, 61/1973;
- Income Tax Act, 58/1962;
- Financial Intelligence Centre Act, 38/2001;
- ECTA, 25/2002;
- RICA, 70/2002;
- Second Hand Goods Act, 23/1955;
- Firearms Control Act, 60/2000;
- Basic Conditions of Employment Act, 75/1997;
- Unemployment Insurance Act, 63/2001;
- Unemployment Insurance Contributions Act, 4/2002;
- National Credit Act, 34/2005;
- Compensation for Occupational Injuries & Diseases Act, 130/1993;
- Skills Development Levies Act, 9/1999;
- Employment Equity Act, 55/1998;
- Labour Relations Act, 66/1995;
- Securities Services Act, 36/2004;
- Value-Added Tax Act, 89/1991;
- POPI, 4/2013;
- PRECCA, 12/2004;
- PROCDATRA, 33/2004;
- FAIS, 37/2002;
- Prescription Act, 68/1969;
- Safex Rules;
- Legal advice (Juta);
- Companies Amendment Act 3/2011;
- Companies Regulations 2011;
- Tax Administration Act, 28/2011.

FORM 2

REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorisation, must be attached to this form.*

TO: The Information Officer

____

____

____

____

(Address)

E-mail address: ____________________

Fax number: ____________________

Mark with an ***"X"***

☐ Request is made in my own name ☐ Request is made on behalf of another person.

PERSONAL INFORMATION				
Full Names				
Identity Number				
Capacity in which request is made *(when made on behalf of another person)*				
Postal Address				
Street Address				
E-mail Address				
Contact Numbers	Tel. (B):		Facsimile:	
	Cellular:			
Full names of person on whose behalf request is made *(if applicable):*				
Identity Number				

Postal Address				

Street Address				
E-mail Address				
Contact Numbers	Tel. (B)		Facsimile	
	Cellular			
PARTICULARS OF RECORD REQUESTED *Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located.* (*If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)*				
Description of record or relevant part of the record:				
Reference number, if available				
Any further particulars of record				
TYPE OF RECORD *(Mark the applicable box with an "**X**")*				
Record is in written or printed form				
Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*				
Record consists of recorded words or information which can be reproduced in sound				

Record is held on a computer or in an electronic, or machine-readable form	

FORM OF ACCESS *(Mark the applicable box with an "**X**")*	
Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)*	
Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)*	
Transcription of soundtrack *(written or printed document)*	
Copy of record on flash drive *(including virtual images and soundtracks)*	
Copy of record on compact disc drive*(including virtual images and soundtracks)*	
Copy of record saved on cloud storage server	

MANNER OF ACCESS *(Mark the applicable box with an "**X**")*	
Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)*	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format *(including transcriptions)*	
E-mail of information *(including soundtracks if possible)*	
Cloud share/file transfer	
Preferred language *(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)*	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED *If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.*	
Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a) A request fee must be paid before the request will be considered. *b) You will be notified of the amount of the access fee to be paid.* *c) The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.* *d) If you qualify for exemption of the payment of any fee, please state the reason for exemption*	
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	**Facsimile**	**Electronic communication** ***(Please specify)***

Signed at______________________this_____________day of__________________20 ___________

____

Signature of Requester / person on whose behalf request is made

---

FOR OFFICIAL USE

Reference number:	
Request received by: *(State Rank, Name And Surname of Information Officer)*	
Date received:	
Access fees:	
Deposit (if any):	

____

Signature of Information Officer

ANNEXURE B

PAIA PRESCRIBED FEES

The following applies to requests (other than personal requests):

A requestor is required to pay the prescribed fees (R50.00) before a request will be processed;

If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which will be payable if the request were granted);

A requestor may lodge an application with the court against the tender/payment of the request fee and / or deposit;

Records may be withheld until the fees have been paid.

Payments should be made Zak Steel Corporation Proprietary Limited

FEES IN RESPECT OF PRIVATE BODIES

1. The fee for a copy of the manual as contemplated in regulation 9(2) (c) is R1,10 for every photocopy of an A4-size page or part thereof.
2. The fees for reproduction referred to in regulation 11(1) are as follows:
   a. For every photocopy of an A4-size page or part thereof R 1,10
   b. For every printed copy of an A4-size page or part thereof held on a computer or in an electronic or machine readable-form R 0,75
   c. For a copy in a computer-readable form on – i. stiffy disc R7,50 ii. compact disc R70,00
   d. For a transcription of visual images:
      i. for an A4-size page or part thereof R40,00
      ii. For copy of visual images R60,00
   e. For transcription of an audio record:
      i. for an A4-size page or part thereof R20,00
      ii. For a copy of an audio record R30,00
3. The request fee payable by the requester, other than a personal requester, referred to in regulation 11(2) R50,00
4. The access fees payable by the requester referred to in regulation 11(3) are as follows:
   a. For every photocopy of an A4-size page or part thereof R1,10
   b. For every printed copy of an A4-sized page or part thereof held on a computer or in a electronic or machine-readable form R0,75
   c. For copy in a computer readable form on:
      i. stiffy disc R7,50
      ii. compact disc R70,00
   d. For a transcription of visual images:
      i. for an A4-size page or part thereof R40,00
      ii. For a copy of visual images R60,00
   e. For a transcription of an audio record:
      i. for an A4-size page or part thereof R20,00
      ii. For a copy of an audio record R30,00
   f. To search for and prepare the record for disclosure R30,00 p/h or part of
5. For purposes of section 54(2) of the Act, the following applies:
   a. Six hours as the hours to be exceeded before a deposit is payable; and
   b. one third of the access fee is payable as a deposit by the requester.
6. The actual postage is payable when a copy of a record must be posted to a requester.