MSP Mine Support Products (Pty) Ltd

108 Houtkop Road

Duncanville

Vereeniging 1930

Tel: +27 (0)16 100 0855

Co Reg No. 2020/170666/07

VAT No. 4060292234

www.msp.co.za

MSP Mine Support Products (Pty) Ltd
Reg. No. 2020/170666/07

Protection of Personal Information Act "POPI"

Policies

Last updated: 30 June 2021

POLICY

1. Introduction

The Company is an organisation that always strives to comply with all South African law and recognises that a person's (including employees, customers and suppliers) Constitutional right to privacy is of the upmost importance, therefore the protection of personal information is vital for sustainability and growth of the business.

2. Purpose

The purpose of this policy is to incorporate the requirements of the Protection of Personal Information Act No. 4 of 2013 (hereafter called the Act) into the everyday operations of the Company and to ensure that these requirements are documented and implemented in the Company to ensure full compliance and adherence to the Act.

3. Scope

This scope of this policy applies to all directors, shareholders, members, managers, supervisors and employees, i.e. to all staff employed on a casual, contractual or permanent basis.

4. Objectives

The Company and its employees shall adhere to this policy in the handling of all personal information received from, but not limited to natural persons, employees, clients, suppliers, agents, representatives and business partners to ensure compliance with this Act, applicable regulations and other rules relating to the protection of personal information.

The objectives of this policy are:

- Emphasise the company's commitment to ethics and the rule of law.
- To establish a set of uniform rules and regulations which are of a high ethical and legal standard.
- To create a framework, without uncertainty, within which the employees can operate in accordance with the Act.
- To create a structure which allows the prevention and/or detection of wrongdoing.

- To provide clear processes and procedures without ambiguity.
- To protect the interests of both the company and the data subject.
- To balance the right of privacy against other rights, particularly the right of access to information.
- The implementation of corrective action where the Company and/or its employee's actions are unacceptable or do not meet the required standards with regards to the Act.

5. Definitions and Interpretation

In this Policy, unless the context otherwise indicates:

"data subject": means the person to whom personal information relates;

"direct marketing": means to approach a data subject, either in person or by email 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 service to the data subject; or

b) Requesting the data subject to make a donation of any kind for any reason.

"electronic communication": means any text, date, data, voice, sound or image message sent over an electronic communications network which is stored in the network or the recipient's terminal equipment until it is collected by the recipient.

"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.

"information officer": of, or in relation to, a –

a) Private body means the head of a private body as contemplated in Section 1 of the Promotion of Access to Information Act.

"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;

"person": means a natural person or a juristic person.

"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, 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 would reveal the contents of the original correspondence if the message is of a personal or confidential nature;

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.

"private body": means –

a) A natural person who carries or has carried on any business or profession, but only in such capacity;

b) A partnership which carries or has carried on any trade, business or profession; or

c) Any former or existing juristic person but excludes a public body.

"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.

"Promotion of Access to Information Act": means the Promotion of Access to Information Act, 2000 as amended;

"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 provincial constitution; or

II. Exercising a public power or performing a public function in terms of any legislation.

"public record": means a record that is accessible in the public domain and which is in the possession od or under the control of a public body, whether or not it was created by that public body.

"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 recorded, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

III. Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

IV. Book, map, plan, graph or drawing;

V. Photograph, film, negative, tape or other device in which one or more visuals 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; and

c) Regardless of when it came into existence.

"regulator": means the Information Regulator established in terms of Section 39.

"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 reasonable foreseeable method to identify the data subject; or

c) Can be linked by a reasonable foreseeable method to other information that identifies the data subject, and **'re-identified'** has a corresponding meaning.

"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.

"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.

"special personal information": means personal information as referred to in Section 26 of this Act.

"the Act": means the Protection of Personal Information Act, No. 4 of 2013.

"this Policy": means this document including all policies, procedures, addendums, annexures attached hereto or incorporated by reference.

"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.

In this Code, unless expressly stated otherwise or where the context indicates otherwise, words in the singular shall also mean the plural and other way round, words in the masculine also mean the feminine and the neuter, and words referring to a natural person shall include a reference to a body corporate and the other way around.

The clause headings in this agreement have been inserted for convenience only and will not be taken into consideration in its interpretation.

The *contra proferentem* rule shall not apply, which shall mean that this agreement and its provisions shall not be adversely interpreted as against the party that drafted such Agreement.

The *iusdem generis* rule shall not be applicable, which means that when the words "including" followed by specific examples are utilised, such examples shall not be interpreted nor construed as to limit the ambit of the relevant clause of this Agreement.

The words “will”, “shall, and “must” utilised in a set of circumstances that imposes any obligation or restriction on any Party shall have an identical meaning.

6. Key principles

The Company, its employees are committed to the following principles:

- To give effect to the Constitutional right to privacy, by safeguarding personal information when processed by the Company, subject to justifiable limitations;
- To regulate the manner in which personal information may be processed, by establishing conditions, in agreement with international standards, that prescribe the minimum requirements for the lawful processing of personal information;
- To be transparent in its standard operating procedures that govern the processing of personal information;
- To comply with the applicable legal and regulatory requirements regarding the processing of personal information;
- To collect personal information through lawful and fair means and to process personal information in a manner compatible with the purpose for which it was collected;
- Where required by law and according to local requirements. To inform data subjects when personal information is collected about them;
- Where required by law, regulations or guidelines, to obtain a data subject’s consent prior to processing his/her/its personal information;
- To strive to keep personal information accurate, complete, up-to-date and reliable for its intended use;
- To strive to develop reasonable security safeguards against risk, losses, unauthorized access, destruction, use, modification or disclosure of personal information;
- To strive to provide data subjects with the opportunity to access the personal information relating to them and, where applicable, to comply with requests to correct, amend or rectify the personal information where incomplete, inaccurate or not compliant with the standard operating procedures;
- To only share personal information, such as permitting access, transmission or publication, with third parties (either within or outside the Company), only if

reasonable assurance can be provided that the recipient of such information will apply suitable privacy and security protection to the personal information;

7. Procurement of Personal Information

7.1 Personal information collected by the Company and/or any of its representatives, will be collected directly from the data subject, unless:

a) The information is contained or derived from a public record or has deliberately been made public by the data subject;

b) The data subject or a competent person where the data subject is a child, has consented to the collection of the information from another source;

c) Collection of the information from another source would not prejudice a legitimate interest of the data subject;

d) Collection of the information from another source is necessary:

I. To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

II. To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

III. For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

IV. To maintain the legitimate interests of the Company or of a third party to whom the information is supplied;

e) Compliance would prejudice a lawful purpose of the collection; or

f) Compliance is not reasonably practicable in the circumstances of the particular case.

7.2 Personal Information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the Company.

7.3 Steps will be taken to ensure that the data subject is aware of the purpose of the collection of the information.

7.4 The Company will take reasonably practicable steps to ensure that the personal information is complete, accurate, not missing and updated where necessary,

having regard to the purpose for which the personal information is collected and further processed.

7.5 Where personal information is collected from a data subject, the Company will take reasonable practicable steps to ensure that the data subject is aware of:

7.5.1 The information being collected and where the information is not collected from the data subject, the source from which it is collected;

7.5.2 The name and address of the Company;

7.5.3 The purpose for which the information is being collected;

7.5.4 Whether or not the supply of the information by the data subject is voluntary or mandatory;

7.5.5 The consequences of failure to provide the information;

7.5.6 Any particular law authorising or requiring the collection of the information;

7.5.7 The fact that, where applicable, the Company intends to transfer the information to a third country or international organisation and the level of protection offered to the information by that third country or international organisations;

7.5.8 Any further information such as the:

7.5.8.1 Recipient or category of recipients of the information;

7.5.8.2 Nature or category of the information;

7.5.8.3 Existence of the right of access to and the right to rectify the information collected;

7.5.8.4 Existence of the right to object to the processing of personal information;

Which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

7.6 The steps referred to in clause 7.5 must be taken:

7.6.1 If the information is collected directly from the data subject, prior to the information being collected, unless the data subject is already aware of the information as referred to in clause 7.5;

7.6.2 In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

7.7 It will not be necessary for the Company to comply with clause 7.5 if:

7.7.1 The data subject or a competent person if the data subject is a child has provided consent for the non-compliance;

7.7.2 Non-compliance would not prejudice the legitimate interests of the data subject;

7.7.3 Non-compliance is necessary:

7.7.3.1 To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

7.7.3.2 To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

7.7.3.3 For the conduct of proceedings in any court or tribunal that have commenced or are reasonable contemplated; or

7.7.3.4 In the interest of national security.

7.7.4 Compliance would prejudice a lawful purpose of the collection;

7.7.5 Compliance is not reasonably practicable in the circumstances of the particular case; or

7.7.6 The information will:

7.7.6.1 Not be used in a form in which the data subject may be identified; or

7.7.6.2 Be used for historical, statistical or research purposes.

8. Processing of Personal Information

8.1 Personal Information will only be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

8.2 Personal Information may only be processed if:

8.2.1 given the purpose for which it was processed, it is adequate, relevant and not excessive;

8.2.2 the data subject or a competent person where the data subject is a child consents to the processing;

8.2.3 processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party;

8.2.4 processing complies with an obligation imposed by law on the Company;

8.2.5 processing protects a legitimate interest of the data subject; or

8.2.6 processing is necessary for pursuing the legitimate interest of the Company or of a third party to whom the information is supplied.

8.3 In the event that the Company appoints or authorises an operator to process any personal information on its behalf or for any reason, it will implement necessary agreements to ensure that the operator or anyone processing personal information on behalf of the Company or an operator, must:

8.3.1 Process such information only with the knowledge or authorisation of the Company; and

8.3.2 Treat personal information which comes to his/her/its knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of his/her/its duties.

8.4 The Company must maintain the documentation of all processing operations under its responsibility.

9. Further Processing of Personal Information

9.1 The Company must ensure that the further processing of personal information be compatible with the purpose for which it was collected.

9.2 To assess whether further processing is compatible with the purpose of collection, the Company will take account of:

9.2.1 The relationship between the purpose of the intended further processing and the purpose for which the information was collected;

9.2.2 The nature of the information concerned;

9.2.3 The consequences of the intended further processing for the data subject;

9.2.4 The manner in which the information has been collected; and

9.2.5 Any contractual rights and obligations between the parties.

9.3 The further processing of personal information will not be incompatible with the purpose of collection if:

a) The data subject or competent person where the data subject is a child, has consented to the further processing of the information;

b) The information is available in or derived from a public record or has deliberately been made public by the data subject;

9.3.1 Further processing is necessary:

a) To avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

b) To comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue;

c) For the conduct of proceedings in any court or tribunal that have commenced or are reasonable contemplated; or

9.3.2 The further processing of the information is necessary to prevent or mitigate a serious and imminent threat to:

a) Public health or public safety; or

b) The life or health of a data subject or other individual(s);

9.3.3 The information is used for historical, statistical or research purposes and The Company ensures that the processing is carried out solely for such purposes and will not be published in an identifiable form.

10. Retention and Restriction of Records

10.1 Records of personal information must not be retained any longer than necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

10.1.1 The retention of a record is required or authorized by law;

10.1.2 The Company reasonable requires a record for lawful purposes related to its functions or activities;

10.1.3 Retention of a record is required by a contact between the parties thereto; or

10.1.4 The data subject or a competent person where the data subject is a child has consented to the retention of a record.

10.2 Information collected or processed initially for the purposed of historical, statistical or research value, may be retained for a period longer than contemplated in clause 10.1, providing the Company has appropriate measures in place to safeguard these records against uses other than what it was intended for initially.

10.3 The Company will destroy or delete a record of personal information or de-identify it as soon as reasonably practicably after The Company is no longer authorized to retain a record.

10.4 The de-identifying or deletion of a record of personal information must be done in a manner that prevents its reconstruction in an intelligible/understandable form.

10.5 In the event that The Company uses a record of personal information of a data subject to make a decision about the data subject, it must:

10.5.1 Retain the record for such period as may be required or prescribed by law or a code of conduct; or

10.5.2 If there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

10.6 The Company will restrict the processing of personal information if:

10.6.1 Its accuracy is contested by the data subject, for a period enabling The Company to verify the accuracy of the information;

10.6.2 The Company no longer needs the personal information for achieving the purpose for which it was collected or subsequently processed, but it has to be maintained for purposed of proof;

10.6.3 The processing is unlawful, and the data subject opposed its destruction or deletion and request the restriction of its use instead; or

10.6.4 The data subject requests to transit the personal data into another automated processing system.

10.7 Personal information that has been restricted may only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person where the data subject is a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

10.8 Where the information is restricted, The Company will inform the data subject before lifting the restriction.

11. Security Safeguards

11.1 The Company will secure the integrity and confidentiality or personal information in its possession or under its control by taking appropriate, reasonable, technical and organisational measures to prevent:

11.1.1 Loss of, damage to or unauthorized destruction of personal information; and

11.1.2 Unlawful access to or processing of personal information.

11.2 The Company will take reasonable measures to:

11.2.1 Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

11.2.2 Establish and maintain appropriate safeguards against the risks identified;

11.2.3 Regularly verify that the safeguards are effectively implemented; and

11.2.4 Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

11.3 The Company will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

11.4 The Company will, in terms of a written contract between The Company and the operator, ensure that he operator which processes personal information for The Company, establishes and maintain security measures.

11.5 The operator will inform The Company immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorized person.

12. Security Compromises

12.1 Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by nay unauthorized person, The Company will notify:

12.1.1 The Information Regulator; and

12.1.2 The data subject, unless the identity of such data subject cannot be established.

12.2 The notification of a breach will be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of The Company's information system.

12.3 The Company will only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

12.4 The notification to a data subject will be in writing and communicated to the data subject in at least one of the following ways:

12.4.1 Posted to the data subject's last known physical or postal address; or

12.4.2 Sent by e-mail to the data subject's last known e-mail address; or

12.4.3 Placed in a prominent position on the website of The Company; or

12.4.4 Published in the news media.

12.5 The notification will provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including:

12.5.1 A description of the possible consequences of the security compromise;

12.5.2 A description of the measures that The Company intends to take or has taken to address the security compromise;

12.5.3 A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

12.5.4 If known to The Company, the identity of the unauthorized person who may have accessed or acquired the personal information.

13. Rights of the Data Subject

13.1 The data subject or competent person where the data subject is a child, may withdraw his, her or its consent to procure and process his, her or its personal information, at any time, providing the lawfulness of the processing of the personal information before such withdrawal or the processing of personal information in terms of clause 9 is not affected.

13.2 A data subject may object, at any time, to the processing of personal information:

13.2.1 In terms of clause 9 in writing, on reasonable grounds relating to his/hers or its particular situation, unless legislation provides for such processing; or

13.2.2 For purposes of direct marketing other than direct marketing by means of unsolicited electronic communications.

13.3 A data subject, having provided adequate proof of identity, has the right to:

13.3.1 Request the Company to confirm, free of charge, whether or not the Company holds personal information about the data subject; and

13.3.2 Request from The Company a record or a description of the personal information about the data subject held by The Company, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information:

13.3.2.1 Within a reasonable time;

13.3.2.2 At a prescribed fee as determined by the Information Officer;

13.3.2.3 In a reasonable manner and format; and

13.3.2.4 In a form that is generally understandable.

13.4 A data subject may, in the prescribed manner, request The Company to:

13.4.1 Correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

13.4.2 Destroy or delete a record of personal information about the data subject that The Company is no longer authorized to retain.

13.5 Upon receipt of a request referred to in clause 14.4, The Company will, as soon as reasonably practicable:

13.5.1 Correct the information;

13.5.2 Destroy or delete the information;

13.5.3 Provide the data subject, to his, her or its satisfaction, with credible evidence in support of the information; or

13.5.4 Where an agreement cannot be reached between The Company and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will

always be read with the information, an indication that a correction of the information has been requested but not been made.

13.6 The Company will inform the data subject, who made a request, of the action as a result of the request.

14. Request for Disclosure

The Company will respond promptly when the data subjects request notification of purpose of use, disclosure, correction, addition or deletion of details, and suspension of use or elimination relating to personal information held by the Company.

15. Monitoring and Enforcement

Each employee of the Company, who is deemed an Operator, will be responsible for administering and overseeing the implementation of this policy and, as applicable, supporting guidelines, standard operating procedures, notices, consents and appropriate related documents and processes. Managers and responsible employees will be trained according to the functions in legal requirements, policies and guidelines that govern the protection of personal information in The Company. The Company will conduct periodic reviews and audits, where appropriate, to demonstrate compliance with privacy law and its policies, this Act and any applicable regulations. Employees who violate the guidelines and standard operating procedures of this policy may be subject to disciplinary action being taken against him/her which may lead to dismissal.

16. Point of Contact

The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the handling, collection, processing or re-identifying of personal information shall be directed to the Information Officer or Deputy Information Officer(s) as referred to in the Information Officer Policy.

17. Standard Operating Procedures

Each department will establish appropriate privacy standard operating procedures that are consistent with this policy, local customs and practices as well as legal and regulatory requirements.