Vedanta Zinc International

Data Subject Access Request Policy

VZI Doc #	SBU Doc #	Document Type	Review Status
VZI-PIA-GEN-POL-0014	[SBU_DocNo]	Policy	Approved
Version	**Confidentiality Level**	**Audit Standard**	**HOD**
2	Public (C4)	POPIA	Hermien Uys

Effective Date	Review Date	Review Cycle	Next Review Date
3-30-2023	5-17-2023	1 Year	3-29-2024

Content Owner(s)
Loganathan Govender (Company Secretary & Compliance Officer | VZI)

Content Reviewer(s)
[txtReviewers]

Content Approver(s)
Hermien Uys (Head: Legal | VZI) || Pushpender Singla (Executive Director and Chief Financial Officer | VZI)

❖ Change History

Modified Date	Version	Modified by	Description of change
2021/06/01	1.0	Hermien Uys	Sent for approval
2023/03/23	1.1	Leonard Matthews	Sent for comments
2023/03/30	2.0	Leonard Matthews	Sent for approval

Table of Contents

❖ Definitions and Abbreviations

Word / Phrase / Abbreviation	Definition

1. Introduction

Black Mountain Mining (Pty) Ltd ("BMM") is required to comply with the requirements of the Protection of Personal Information Act No. 4 of 2013 ("POPIA") which gives data subjects the right to ask for a description of the personal information that BMM holds about them.

2. Application and Consequences of Non-Compliance with This Policy

2.1. This policy applies to all staff of BMM, which includes all permanent and temporary staff, contractors, and agency workers who are subject to the conditions and scope of this policy. Failure to comply may lead to disciplinary action, including dismissal or termination of contract or engagement (as appropriate) for serious or repeated breaches of this policy.

2.2. It may also be the case that your conduct and or action(s) may be unlawful and BMM reserves the right to inform the appropriate authorities. Action(s) may result in civil or criminal proceedings. Staff should note that in some cases they may be personally liable for their actions and or conduct.

3. Purpose of This Document

3.1. This document outlines the process for dealing with Subject access requests that are received by BMM and covers:

3.2. How to identify a Subject Access Request;

3.3. Who is entitled to make one;

3.4. Who within BMM is responsible for dealing with them;

3.5. The timescale for responding to one;

3.6. How to assess whether a Subject Access Request is valid;

3.7. How to set the scope of, and conduct any search for, information in response to a Subject Access Request;

3.8. What information should be provided in response to the Subject Access Request; and

3.9. What information may be withheld from a response to the Subject Access Request?

3.10. This document provides guidance only and in the event of a Subject Access Request please contact the Information Officer ("IO") immediately - please see the list at the end of the note for contact details of the IO.

4. Receipt of Subject Access Requests

4.1. A Subject Access Request may be received by BMM in any of a number of different forms, including a telephone call, email or letter requesting access to personal information. Subject Access Requests generally tend to originate from current or past employees, job applicants, clients or third parties acting on their behalf (particularly where criminal or civil proceedings are involved).

4.2. In the first instance, it may not always be clear that a data subject is making a Subject Access Request. Therefore, it is important to be familiar with this policy to be able to identify a Subject Access Request.

4.3. If you receive what you believe to be a Subject Access Request in any form then it is important that you forward a copy of the request to the IO immediately, who will manage the Subject Access Request.

4.4. In the case of a telephone call, it is best practice to inform the data subject that his/her/its request for information must be made in writing and cannot be processed otherwise. You should also notify the IO that the phone call has taken place.

4.5. Once you have passed the request on to the IO and have received an acknowledgement that it has been received, responsibility for processing the Subject Access Request will be managed by the IO and individuals from the relevant department within BMM (as applicable).

5. Time Period for The Response

5.1. BMM must respond to a valid Subject Access Request within a reasonable period but always within 30 days.

5.2. Where a Subject Access Request is missing any of its required elements, it is essential that a prompt request for the missing part(s) is sent back to the data subject asking for the missing elements.

5.3. Once all of the requirements set out above have been met and the request has become a valid Subject Access Request, the stated period for providing a formal response must be complied with.

6. Who Is Entitled to Make a Subject Access Request?

6.1. Any data subject is entitled to make a Subject Access Request to BMM. BMM will typically receive Subject Access Requests:

6.1.1. from its employees or former employees or job applicants;

6.1.2. from an individual working for a supplier or a supplier;

6.1.3. from a customer who is an individual or a customer; or

6.1.4. From an individual that has used BMM website.

6.2. These individuals and entities have a right to be informed by BMM whether personal information about them is being processed. If personal information is being processed in almost any way by BMM then the data subject is entitled to be given any of the following information:

6.2.1. a description of the personal information held; and

6.2.2. An indication of all the third parties or categories of third parties who have or have had of access to the information.

Validity of a Subject Access Request

6.3. It is necessary to confirm that the Subject Access Request is valid. The validity of a Subject Access Request will depend on the format and content of the Request. A valid Subject Access Request:

6.3.1. is in writing to BMM physical or postal address, fax number or e-mail address;

6.3.2. provides sufficient information to allow the identification of the data subject in requesting the personal information and the information requested;

6.3.3. indicates the form in which the information should be provided;

6.3.4. specifies an address, fax number or email address of the data subject in South Africa; and

6.3.5. Includes sufficient identification of the data subject to which the Subject Access Request relates.

6.3.6. specifies an address, fax number or email address of the data subject in South Africa; and

6.3.7. Includes sufficient identification of the data subject to which the Subject Access Request relates.

7. Identification and Search Terms

7.1. The IO must confirm the identity of the data subject making the request - i.e. to confirm the person is who the person says it is.

7.2. Where the Subject Access Request is made by an employee or a former employee then this will normally be straightforward. The information to be requested will usually be the employee's/former employee's:

- Employee ID;
- Department;
- Room or Desk number; and / or
- Employee's telephone extension.

7.3. Where the Subject Access Request is made by someone other than an employee or a former employee then you should send a letter requesting confirmation of identity and also requesting, if necessary, further information to be provided to assist in focusing the search for information.

8. Setting The Scope and Conducting the Search

8.1. Subject Access Requests sometimes clearly identify specific information sought by the data subject. This permits a simple and targeted search for that information.

8.2. However, other requests are expressed more widely and may, for example, simply request all information held about them (e.g. "Please send me a copy of all the information you have on me"). Such a wide-ranging request would be difficult and onerous to comply with given the volume of information that would have to be reviewed.

8.3. When a wide-ranging request is made then the first step is always to contact the data subject and try to obtain clarifications about the information that they actually want. This may often result in a much more specific request leading to a much more targeted search.

8.4. Typically, requests may focus on copies of interview notes, employment application forms, personnel files, appraisal information, and holiday and leave information, CCTV footage and emails. However, if the data subject is not prepared to focus their request then you should use the "Default BMM Search Parameters" set out below.

8.5. In most cases:

8.5.1. the search should include any centrally-held personnel files about the data subject (such as BMM employee personnel file);

8.5.2. General and non-specific requests (e.g. for the provision of "all" information held about a data subject) are not acceptable. The request must relate to specific personal information;

8.5.3. If the search relates to emails, then it should only apply to a limited number of email accounts over a limited period. Keyword searching may also be used; and

8.5.4. It is not necessary to restore back-up information in order to respond to the request unless the data subject has a real need for specific information contained in the back-ups.

8.5.5. In general, when setting the parameters for a search, you must consider whether this constitutes a reasonable and proportionate search. This will generally depend on the circumstances but you should consider:

8.5.6. The likelihood that the information exists (i.e. is it just a "fishing expedition"?);

8.5.7. The value or importance of the information to the data subject;

8.5.8. The cost of locating and reviewing the information; and

8.5.9. Whether the information is intended for use in litigation (while pending litigation doesn't invalidate a Subject Access Request, it may be more appropriate for disclosure to be made during discovery).

9. The Default Search Parameters for BMM

9.1. The Default Search Parameters attempt to take into account the above to provide a reasonable and proportionate response so searches for a general request for access to personal information should generally be based on the following parameters (noting that the specific facts on each request may dictate other search factors), however this may vary from request to request:

9.1.1. A copy of the data subject's personnel file should be provided (in the case of an employee or a former employee);

9.1.2. Pre-defined keywords should be used to search email;

9.1.3. There should be no restoration of back up data without the prior approval of the IO.

9.2. It is important to note that any emails sent internally about the Subject Access Request itself will usually not need to be included in the response, on the basis that they may be legally privileged.

10. IT Department Assistance for Electronic Records

10.1. The search may require the assistance of other departments, such as the IT department for tracking.

10.2. The IO should define a specific form to be used when requesting assistance from other department, which should set out clearly:

10.2.1. the names of the inbox owners;

10.2.2. the date range (no longer than [6 months] from the date that the valid Subject Access Request was received); and

10.2.3. Relevant search terms and parameters.

11. Which Information That Is Found in The Search Must Be Disclosed and What Can BMM Refuse to Disclose?

11.1. A Subject Access Request only entitles the data subject to access personal information about himself/herself. In general, personal information about a data subject is required to be disclosed if it identifies that data subject.

11.2. However, there are important exemptions which may apply. These exemptions apply to very specific information and are complex in its interpretation. The IO will analyses the retrieved personal information and shall apply any relevant exemption.

11.3. Such exemptions are set out in our PAIA manual and may, for example, include information:

11.3.1. That is subject to legal professional privilege; or

11.3.2. That reveals the identity of a third party data subject.

12. Other Information to Be Included In The Response

The data subject is also entitled to information about the third parties or categories of third parties who have or have had access to his / her personal information.

13. Consequences of Non-Compliance

It is essential that all staff comply with all relevant parts of this policy. Any failure to comply with this policy could have serious consequences for BMM and its employees. Failure to comply may lead to: disciplinary action, including dismissal for serious or repeated breaches; civil or criminal proceedings; and/or personal liability for those responsible.

14. Policy Revision

This policy has been reviewed and approved by the IO, and is subject to change without prior notice.

15. Contact Details of The IO

15.1. Name: Pushpender Singla
15.2. Address: p/a BMM, 1 Penge Road, Aggeneys, Northern Cape, South Africa
15.3. E-mail address: PSingla@vedantaresources.co.za
15.4. Telephone number: +27 011 685 3963

16. Review and Approval

Content Owner(s)
Loganathan Govender (Company Secretary & Compliance Officer | VZI) TimeStamp: 2023/03/31 11:39:41 AM

Content Reviewer(s)
[txtRew2]

Content Approver(s)
Hermien Uys (Head: Legal | VZI) TimeStamp: 2023/03/31 12:05:36 PM || Pushpender Singla (Executive Director and Chief Financial Officer | VZI) TimeStamp: 2023/05/17 02:20:44 PM

This document was approved (in sequence) by the individuals above using electronic approval in our Document Control System.

Final approval status: Approved

Approvals were done electronically.

❖ Annexures / Appendix