Data Subject Access Request Policy

1. Introduction

1.1 The Company needs to keep certain information about its employees and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the Company must comply with the Data Protection Principles. In summary these state that personal data shall:

i) be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

ii) be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.

iii) be adequate, relevant and not excessive for those purposes.

iv) be accurate and kept up to date.

v) not be kept for longer than is necessary for that purpose.

vi) be processed in accordance with the data subject's rights.

vii) be kept safe from unauthorised access, accidental loss or destruction.

1.2 The Company and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the Company has developed the Data Protection Policy.

1.3 This policy provides guidance for staff members on how data subject access requests should be handled, and is intended for internal use. It is not a privacy policy or statement, and is not to be made routinely available to third parties.

1.4 This policy applies to all staff but much of it is aimed primarily at those members of staff who are authorised to handle data subject access requests. These sections are identified by the words '(authorised staff)' appearing in the section title. For other staff members, it provides guidance on:

I. what to do if the employee receive a data subject access request;

II. and how to decide whether a request for information is a data subject access request

2. **How to recognise a data subject access request**

2.1 A data subject access request is a request from an individual (or from someone acting with the authority of an individual):

i. for confirmation as to whether the company process personal data about him or her and, if so
ii. for access to that personal data
iii. and certain other supplementary information

2.2. Such a request should be made in writing.

2.3 All data subject access requests should be immediately directed to the following email address: info@csgrecruit.co.za

3. **What to do when the employee or Agent receive a data subject access request**

3.1 If the employee or agent receive a data subject access request and the employee are not authorised to handle it, the employee must immediately take the steps set out below. All staff members should take that note that there are limited timeframes in which to respond to Data Subject Request and should forward and/or act on the requests immediately.

3.2 If the employee or agent are in any way unsure as to whether a request for information is a data subject access request, please contact the Information Officer.

3.3 If the employee or agent receive a data subject access request by email, the employee must immediately forward the request to this email address: info@csgrecruit.co.za

3.4 If the employee or agent receive a data subject access request by letter the employee must send a scanned copy of the letter to this email address info@csgrecruit.co.za or when applicable hand the letter over directly to the Information Officer.

3.5 In the event that information is forwarded via email the employee or agent will receive confirmation when the request has been received. If the employee do not receive such confirmation within 2 (two) working days of sending it, the employee should contact the Information Officer to confirm safe receipt.

3.6 The employee or agent must not take any other action in relation to the data subject access request. The Information Officer will advise the employee if any further action from their side is required.

4. Conditions for responding to a valid request

4.1 Where the company process a large quantity of information about an individual, the company may need to ask the individual to specify the information or processing activities to which the request relates.

4.2 The company will not usually charge a fee for responding to a data subject access request. The company may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

i. that is manifestly unfounded or excessive, e.g. repetitive; or

ii. for further copies of the same information.

5. **Identifying the data subject**

5.1 Before responding to a data subject access request, the company will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward.

5.2 The company will not retain personal data for the sole purpose of being able to react to potential data subject access requests in the future.

5.3 If the company have doubts as to the identity of the person making the data subject access request, the company may ask for additional information to confirm his or her identity. Typically the company will request a copy of the individual's ID/drivers licence/passport to enable them to establish his or her identity.

5.4 If, having requested additional information, the company are still not in a position to identify the data subject, the company may refuse to act on a data subject access request.

6. **Refusing to respond to a request**

6.1 The company may refuse to act on a data subject access request where:

I even after requesting additional information in accordance with paragraph 5.4, the company are not in a position to identify the individual making the data subject access request;

ii requests from an individual are manifestly unfounded or excessive, e.g. because of their repetitive character or, in certain circumstances, where the request relates to large amounts of data.

6.2 If the company intend to refuse to act on a data subject access request, the company will inform the individual no later than 2 (two) weeks after receiving his or her request:

I of the reason(s) why the company are not taking action; and

II that they have the right to complain to the Data Protection Officer and/or Regulatory Body.

7. Time limit for responding to a request

7.1 Once a data subject access request is received, the Company must provide the information requested without delay and at the latest within 2 (two) weeks of receiving the request. The employee should therefore make a note of when request was received and when the time limit will end.

7.2 If a data subject access request is complex or the data subject has made numerous requests, the Company:

I may extend the period of compliance by a further 2 (two) weeks; and

II must inform the individual of the extension within one month of the receipt of the request, and explain why the extension is necessary.

8. Information to be provided in response to a request

8.1 The individual is entitled to receive access to the personal data the company process about him or her and the following information:

I the purposes for which the company process the data;

II the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations;

III where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period;

IV the fact that the individual has the right:

i to request that the Company rectifies, erases or restricts the processing of his personal data; or

ii to object to its processing;

iii to lodge a complaint with the Information Regulator

iv where the personal data has not been collected from the individual, any information available regarding the source of the data;

v any automated decision the company have taken about him or her, together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

8.2 The information referred to in paragraph 8.1 should be provided using the Company's standard form response to data subject request—right of access:

I in a way that is concise, transparent, easy to understand and easy to access;

II using clear and plain language, with any technical terms, abbreviations or codes explained;

III in a commonly-used electronic format, if the data subject access request was made electronically, unless otherwise requested by the individual;

9. **Automated decision-making**

9.1 If the data subject access request specifically asks for information about the reasoning behind any automated decision that the company have taken in relation to important matters relating to the individual (e.g. performance at work, creditworthiness, reliability or conduct), the company must provide a description of the reasoning involved in that automated decision, subject to the following conditions:

I the automated decision must have constituted the sole basis for the decision;

II in providing a description of the logic the company are not required to reveal any information which constitutes a trade secret (e.g. the algorithm behind a credit scoring system).

9.2 If the Company carries out automated decision-making in relation to an individual, the data subject access request may include a request:

I for information relating to the automated decision;

II for human intervention on the part of the Company, i.e. to ask that an individual with the authority and competence to change the decision should review the automated decision, considering all the available data;

III to express his or her point of view on the automated decision; and/or

IV to contest the automated decision.

9.3 If such a request is received, the Information Officer will ensure that it is dealt with in accordance with the POPIA and other relevant legislation and guidance.

10. **How to locate information**

10.1 The personal data the company need to provide in response to a data subject access request may be located in several of our electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

10.2 Depending on the type of information requested, the employee may need to search all or some of the following:

I electronic systems, e.g. databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data;

II manual filing systems in which personal data are accessible according to specific criteria, e.g. chronologically ordered sets of manual records containing personal data;

III data systems held externally by our data processors, e.g. service providers;

IV occupational health records;

V share scheme information held by share scheme administrator

VI insurance benefit information held by benefit provider

VII data held by external support, consultants etc

10.3 The employee should search these systems using the individual's name, employee number, customer account number or other personal identifier as a search determinant.

11. What is personal data?

11.1 Once the company have carried out the search and gathered the results, the company will need to select the information to be supplied in response to the data subject access request. The individual is only entitled to receive information which constitutes his or her personal data.

11.2 Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, e.g. their name, identification number, location data or online identifier. It may also include personal data that has been pseudonymised (e.g. key-coded), depending on how difficult it is to attribute the pseudonym to a particular individual.

12. Requests made by third parties on behalf of the individual

12.1 Occasionally the company may receive a request for data subject access by a third party (an 'agent') acting on behalf of an individual. These agents may include parents, guardians, legal representatives and those acting under a power of attorney or other legal authority. The agent must provide sufficient evidence that he or she is authorised to act on behalf of the individuals.

13. **Exemptions to the right of subject access**

13.1 In certain circumstances the company may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

I Crime detection and prevention: The company do not have to disclose any personal data which the company are processing for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty. This is not an absolute exemption. It only applies to the extent to which the giving of subject access would be likely to prejudice any of these purposes. The company are still required to provide as much of the personal data as the company able to.

II Protection of rights of others: The company do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information (or that information and any other information that the company reasonably believe the data subject is likely to possess or obtain), unless:

i that other individual has consented to the disclosure of the information to the individual making the request; or

ii it is reasonable to disclose the information to the individual making the request without the other individual's consent, having regard to:

- the type of information that would be disclosed;
- any duty of confidentiality owed to the other individual;
- any steps taken by the controller with a view to seeking the consent of the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.
- Confidential references: The company do not have to disclose any confidential references that the company have given to third parties for the purpose of actual or prospective:
- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

13.2 This exemption does not apply to confidential references that the company receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference),

which means the employee must consider the rules regarding disclosure of third-party data before disclosing the reference.

14. **Deleting personal data in the normal course of business**

14.1 The information that the company are required to supply in response to a data subject access request must be supplied by reference to the data in question at the time the request was received. However, as the company have 2 (two) weeks in which to respond and the company are generally unlikely to respond on the same day as the company receive the request, the company is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data are supplied if such amendment or deletion would have been made regardless of the receipt of the data subject access request.

14.2 The company is, therefore, allowed to carry out regular housekeeping activities even if this means that the company delete or amend personal data after the receipt of a data subject access request. What the company is not allowed to amend or delete data because the company does not want to supply the data.

15. Any questions regarding this Policy should be addressed to the Information Officer.