# PRIVACY POLICY

## 1. Policy Purpose

The purpose of this policy is to protect private information about individuals and to ensure the Company conforms with the *Privacy Act 1988, Privacy Amendment (Private Sector) Act 2000*, and the Australian Privacy Principles.

## 2. Policy Provisions

### 2.1 Collection of Information

Personal information will only be collected for purposes necessary to the functions and activities of the Company.

Personal information will only be collected by means that are permissible by law.

When personal information is collected by the Company, the Company must clearly state:

- the fact that the information is being collected;
- the purposes for which the information is being collected;
- the intended recipients of the information;
- whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information is not provided; and
- the existence of any right of access to, and correction of, the information.

When the Company collects personal information, the Company must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that:

- the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete; and
- the collection of the information does not intrude to an unreasonable extent on the personal affairs of the person to whom the information relates.

Where reasonably possible, the Company will only collect personal information directly from the person and/or their employer to whom the information relates. Frequently this will be collected from completed forms, email, letters or other forms of communication.

### 2.2 Use of Information

The Company will not use the information for a purpose other than that for which it was

collected unless:

- the information collected is relevant to that purpose, is not excessive, and is accurate, up to date and complete; and
- the person to whom the information relates has consented to the use of the information for that other purpose;
- the other purpose for which the information is used is directly related to the purpose for which the information was collected;
- the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person; or
- if so directed by a court of law.

If the Company uses or discloses personal information (for the purposes listed above), it must make a written note of the use of disclosure and of the reason for its disclosure.

### 2.3 Access to Information

Access to personal information includes an opportunity for personnel to inspect records, take notes or obtain a photocopy or computer printout however, this must be in the presence of a senior representative of their employer and a senior PeaK employee.

***Access for the Individual***

The Company will provide a person access to their personal information record upon written request by the person, except:

- in the case of personal information, other than health information (if stored on record), providing access would pose a serious and imminent threat to the life or health of any other person;
- providing access would have an unreasonable impact upon the privacy of other persons;
- the request for access is frivolous or vexatious;
- providing access would reveal the intentions of the organisation in relation to negotiations in such a way as to prejudice those negotiations;
- providing access would be likely to prejudice an investigation of possible unlawful activity;
- denying access is required or authorised by or under law and providing access would be likely to prejudice the outcome of an internal investigation.

If the Company is not required to provide a person with access to the personal information because of one or more of the aforementioned reasons, the Company must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

***Access for others***

The Company will not disclose personal information to anyone or any organisation, unless:

- the disclosure is related to the purpose for which the information was collected,

- the person concerned was reasonably likely to have been aware, or had been notified, that the personal information is usually disclosed to the other person or organisation;
- the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health of any person;
- in relation to some investigations and law enforcement process; and,
- where legislation recognises lawful access by some government agencies.

The Company must provide reasons for denial of access or a refusal to correct personal information if so requested.

### 2.4 Provision of Information

The Company will respond to a relevant person's written and signed request for their personal information as soon as practicable.

The time taken to respond to a person's request for access to information may be influenced by various factors. These may include the method of communication, the type and/or amount of personal information requested, how the personal information is held, if a third party needs to be consulted and how it is to be provided to the individual making the request.

### 2.5 Access and Law Enforcement

***Police***

Requests for information from the police will not be accepted over the telephone. Members of staff receiving written requests for personal information from law enforcement agencies must direct the inquirer to the Manager – Stakeholder Relations.

This procedure does not apply in cases where there is an imminent threat to life or safety. However even then reasonable attempts should be made to discuss the matter with the Manager – Stakeholder Relations. In most other circumstances it may be assumed that the Company will require the issuing of a search warrant or subpoena. Records of all requests and disclosures of personal information to the law enforcement agencies will be kept on file by the Company.

***Government***

Departments such as Centrelink, ATO and ASIO sometimes have a lawful need to access personal information held by the Company. Where this need exists, it is recognised in the legislation which establishes the departments and regulates their functions. While the Company wishes to be cooperative with the Commonwealth, it has a responsibility to the personnel whose private information it may have on file. Therefore, any Commonwealth Department requiring personal information should be informed that the Company will supply personal information only in response to a formal notice under the Department's legislation.

***Subpoenas and court orders***

The personal information held by the Company may be required as evidence in court and

tribunal proceedings. These may be matters which do not involve the Company, or litigation to which the Company is joined as a party. Subpoenas received by the Company must be directed to the Manager – Stakeholder Relations and if necessary, will be further escalated.

### 2.6 Security

The Company will take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

The Company must approve the use of personal computers in the workplace or for the copying or transferring of personal information onto personal computers. At the time of separation from the Company, the Company will take all appropriate steps to identify personal information stored on personal computers and direct and supervise the removal of personal information.

### 2.7 Communication

The Privacy Policy forms part of the Company's policies and procedures manual of which new staff are expected to familiarize themselves with. Compliance with the Company's policies and procedures forms part of all employment contracts executed between the Company and it's employees.

### 2.8 Breach of the Privacy Policy

The Privacy Policy is designed to promote and enhance the confidentiality of PK personnel's private information. A failure to comply with this policy will be viewed seriously and may, in line with the employment and other contract(s) in place at the time, result in disciplinary action, including dismissal and/or termination of contracts.

All personnel must report breaches of this policy to the Manager – Stakeholder Relations.

The Company will use its utmost endeavours to protect all personnel who, in good faith and with good grounds, report breaches of the Privacy Policy.

### 2.9 Grievances

Any grievance arising from the application of these arrangements shall be managed by PeaK. In the interim, any unresolved issue should be raised in the first instance with the relevant supervisor. If the nominated supervisor is unable to resolve the matter, it may be referred to PeaK.

## 3 Revisions made to this Policy

| Date | Major, Minor or Editorial | Description |
|---|---|---|
| None | N/A | N/A |

The Company may make changes to this policy from time to time to improve the effectiveness of its operation. In this regard, any PeaK staff member who wishes to make any comments about this policy may forward their suggestions to the Manager – Stakeholder Relations

## 4 Further Assistance

Any staff member or contractor who requires assistance in understanding this policy should first consult their nominated supervisor who is responsible for the implementation and operation of these arrangements in their work area.

Marnus Bothma
Director
12 March 2020