PRIVACY POLICY

1.0 PURPOSE

To identify and explain the fundamental issues associated with the Privacy Amendment (Private Sector) Act 2000 ("**the Act**") which incorporates the Australian Privacy Principles ("**APPs**") and implications for Bradken when collecting, using, keeping secure and disclosing Personal Information in compliance with the Act.

2.0 SCOPE

This policy describes the APPs and the way in which Bradken businesses maintain and administer essential privacy documentation related to employees, customers, suppliers, competitors and regulators, in compliance with Bradken's Policy Statement and the Act.

3.0 RESPONSIBILITIES

3.1 The **Executive General Managers** are responsible for ensuring that Bradken and each of its Businesses implement procedures to address all APPs related to the Act.

3.2 **Business General Managers** are responsible for:

- ensuring that their Business implements, maintains and periodically audits all processes and procedures associated with the APPs described in clause 6.0;
- implementing an effective complaints handling process which allows the business to identify and address any systemic or ongoing compliance problems, and increase consumer and employee confidence in Bradken's privacy procedures; and
- ensuring staff are suitably trained in the concept of privacy and the application of Bradken's privacy policy.

3.3 **Managers** with responsibility for other employees are required to ensure that Personal Information is retained in a manner that precludes unauthorised access and complies with the requirements of the APPs and Bradken policies and procedures.

3.4 All **Supervisors** are responsible for the identification of privacy documentation and assurance that all such documentation, whether hardcopy or electronic, is handled in accordance with Business operating procedures for privacy.

3.5 **Quality Personnel** are responsible for ensuring that periodic audits are conducted to guarantee that privacy of documentation is maintained in accordance with the Businesses policies and procedures.

3.6 **IT Personnel** are responsible for ensuring that regular reviews of security of electronic equipment are conducted to guarantee that privacy of Personal Information in electronic format is maintained in accordance with the Businesses policies and procedures.

4.0 POLICY STATEMENT

Bradken abides by the Australian Privacy Principals under the Privacy Amendment (Private Sector) Act 2000 and by any of Bradken's documented policies and procedures, which apply to Personal and Sensitive Information held by Bradken. Personal Information held by Bradken relates exclusively to statutory and regulatory corporate obligations, and will only be used for the purpose for which it was collected and will be retained to prevent unauthorised access, modification or disclosure.

5.0 DEFINITIONS

For the purpose of this policy document, the following definitions apply.

- **Personal Information** is information or an opinion that can identify a person.
- **Sensitive Information** is information about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal record, or health information.

6.0 OVERVIEW

The APPs are thirteen principles or rules in the Act about how organisations must handle Personal Information and set the base line standards for privacy protection. Bradken is required to comply with the APPs set out in the Act. The following is an overview of the five parts which incorporate the thirteen APPs.

Part 1 – Consideration of personal information privacy

APP-1 – Open and transparent management of personal information

1.1 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

a. will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

b. will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP-2 – Anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Sub-clause 2.1 does not apply if, in relation to that matter:

a. the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

b. it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Part 2 – Collection of personal information

APP-3 – Collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

a. the individual consents to the collection of the information and:

- if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
- if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

b. sub-clause 3.4 applies in relation to the information.

3.4 This sub-clause applies in relation to sensitive information about an individual if:

a. the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

b. a permitted general situation exists in relation to the collection of the information by the APP entity; or

c. the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

d. the APP entity is an enforcement body and the entity reasonably believes that:

- if the entity is the Immigration Department — the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or
- otherwise — the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

e. the APP entity is a non-profit organisation and both of the following apply:

- the information relates to the activities of the organisation;
- the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

a. if the entity is an agency:

- the individual consents to the collection of the information from someone other than the individual; or
- the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

b. it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

APP-4 – Dealing with unsolicited personal information

4.1 If an APP entity receives personal information and the entity did not solicit the information the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under APP-3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under the sub-clause 4.1.

4.3 If the APP entity determines that the entity could not have collected the personal information and the information is not contained in a Commonwealth record the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-

identified.

4.4 If sub-clause 4.3 does not apply in relation to the personal information, APP-5 to APP-13 apply in relation to the information as if the entity had collected the information under APP-3.

APP-5 – Notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

a. to notify the individual of such matters referred to in following sub-clause as are reasonable in the circumstances; or

b. to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of the above sub-clause are as follows:

a. the identity and contact details of the APP entity;

b. if:

- the APP entity collects the personal information from someone other than the individual; or
- the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

c. if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

d. the purposes for which the APP entity collects the personal information;

e. the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

f. any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

g. that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

h. that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

i. whether the APP entity is likely to disclose the personal information to overseas recipients;

j. if the APP entity is likely to disclose the personal information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3 – Dealing with personal information

APP-6 – Use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

a. the individual has consented to the use or disclosure of the information; or

b. sub-clause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This sub-clause applies in relation to the use or disclosure of personal information about an individual if:

a. the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

- if the information is sensitive information — directly related to the primary purpose; or
- if the information is not sensitive information — related to the primary purpose; or

b. the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

c. a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

d. the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

e. the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This sub-clause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

a. the agency is not an enforcement body; and

b. the information is biometric information or biometric templates; and

c. the recipient of the information is an enforcement body; and

d. the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

a. the APP entity is an organisation; and

b. subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with sub-clause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

a. an APP entity is a body corporate; and

b. the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

a. personal information for the purpose of direct marketing; or

b. government related identifiers.

APP-7 – Direct Marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions — personal information other than sensitive information

7.2 Despite sub-clause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

a. the organisation collected the information from the individual; and

b. the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d. the individual has not made such a request to the organisation.

7.3 Despite sub-clause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:

a. the organisation collected the information from:

- the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
- someone other than the individual; and

b. either:

- the individual has consented to the use or disclosure of the information for that purpose; or
- it is impracticable to obtain that consent; and

c. the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

d. in each direct marketing communication with the individual:

- the organisation includes a prominent statement that the individual may make such a request; or
- the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

e. the individual has not made such a request to the organisation.

Exception — sensitive information

7.4 Despite sub-clause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception — contracted service providers

7.5 Despite sub-clause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

a. the organisation is a contracted service provider for a Commonwealth contract; and

b. the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

c. the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the first organisation) uses or discloses personal information about an individual:

a. for the purpose of direct marketing by the first organisation; or

b. for the purpose of facilitating direct marketing by other organisations;

the individual may:

c. if paragraph (a) applies — request not to receive direct marketing communications from the first organisation; and

d. if paragraph (b) applies — request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

e. request the first organisation to provide its source of the information.

7.7 If an individual makes a request under sub-clause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

a. if the request is of a kind referred to in paragraph 7.6(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and

b. if the request is of a kind referred to in paragraph 7.6(e) — the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

a. the *Do Not Call Register Act 2006*;

b. the *Spam Act 2003*;

c. any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

APP-8 – Cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

a. who is not in Australia or an external Territory; and

b. who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Sub-clause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

a. the entity reasonably believes that:

- the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
- there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

b. both of the following apply:

- the entity expressly informs the individual that if he or she consents to the disclosure of the information, sub-clause 8.1 will not apply to the disclosure;
- after being so informed, the individual consents to the disclosure; or

c. the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

d. a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

e. the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

f. the entity is an agency and both of the following apply:

- the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
- the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

APP-9 – Adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

a. the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

b. sub-clause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

a. the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

b. the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

c. the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

d. a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

e. the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

f. sub-clause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3 This sub-clause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

a. the identifier is prescribed by the regulations; and

b. the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

c. the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4 – Integrity of personal information

APP-10 – Quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

APP-11 – Security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

a. from misuse, interference and loss; and

b. from unauthorised access, modification or disclosure.

11.2 If:

a. an APP entity holds personal information about an individual; and

b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

c. the information is not contained in a Commonwealth record; and

d. the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5 – Access to, and correction of, personal information

APP-12 – Access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access — agency

12.2 If:

a. the APP entity is an agency; and

b. the entity is required or authorised to refuse to give the individual access to the personal information by or under:

- the Freedom of Information Act; or
- any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite sub-clause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access — organisation

12.3 If the APP entity is an organisation then, despite sub-clause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

a. the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

b. giving access would have an unreasonable impact on the privacy of other individuals; or

c. the request for access is frivolous or vexatious; or

d. the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

e. giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

f. giving access would be unlawful; or

g. denying access is required or authorised by or under an Australian law or a court/tribunal order; or

h. both of the following apply:

- the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;
- giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

i. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

j. giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

a. respond to the request for access to the personal information:

- if the entity is an agency — within 30 days after the request is made; or
- if the entity is an organisation — within a reasonable period after the request is made; and

b. give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

a. to give access to the personal information because of sub-clause 12.2 or 12.3; or

b. to give access in the manner requested by the individual; the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting sub-clause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

a. the APP entity is an organisation; and

b. the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

a. the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

c. any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

APP-13 – Correction of personal information

Correction

13.1 If:

a. an APP entity holds personal information about an individual; and

b. either:

- the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
- the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

a. the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

b. the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

a. the reasons for the refusal except to the extent that it would be unreasonable to do so; and

b. the mechanisms available to complain about the refusal; and

c. any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

a. the APP entity refuses to correct the personal information as requested by the individual; and

b. the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under sub-clause 13.1 or 13.4, the APP entity:

a. must respond to the request:
   - if the entity is an agency — within 30 days after the request is made; or
   - if the entity is an organisation — within a reasonable period after the request is made; and

b. must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

7.0 PROCEDURE

The following clauses provide details as to the specific requirements of the Act as it applies to Bradken Businesses. Individual Businesses may develop supplementary procedures and processes, which address the following elements of the Act.

7.1 Transparency

7.1.1 Bradken will set out in a document clearly expressed policies on its management of Personal Information and will make the document available to anyone who asks for it.

7.1.2 On request by a person, Bradken will take reasonable steps to let the person know, generally, what sort of Personal Information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

7.1.3 Bradken will not collect Sensitive Information about an individual unless:

(a) the individual has consented;

(b) the collection is required by law;

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns is physically or legally incapable of giving consent to the collection or physically cannot communicate consent to the collection; or

(d) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

7.1.4 Despite clause 7.1.3, Bradken may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected as required by law, other than the Act, or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind Bradken.

7.1.5 Despite clause 7.1.3, Bradken may collect health information about an individual if:

(a) the collection is necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety;

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained;

(c) it is impracticable for Bradken to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law, other than the Act;

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind Bradken; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A of the Act for the purposes of this clause.

7.1.6 If Bradken collects health information about an individual in accordance with clause 7.1.5, Bradken will take reasonable steps to permanently de-identify the information before Bradken discloses it.

7.2 Anonymity

Wherever it is lawful and practicable, individuals have the option of not identifying themselves when entering transactions with Bradken.

7.3 Collection

7.3.1 Bradken will not collect Personal Information unless the information is necessary for one or more of its functions or activities.

7.3.2 Bradken will collect Personal Information only by lawful and fair means and not in an unreasonably intrusive way.

7.3.3 At or before the time Bradken collects Personal Information about an individual from the individual, it will take reasonable steps to ensure that the individual is aware of:

(a) the fact that he or she is able to gain access to the information;

(b) the purposes for which the information is collected;

(c) the organisations, or the types of organisations, to which Bradken usually discloses information of that kind;

(d) any law that requires the particular information to be collected; and

(e) the main consequences (if any) for the individual if all or part of the information is not provided.

7.3.4 If it is reasonable and practicable to do so, Bradken will collect Personal Information about an individual only from that individual.

7.3.5 If Bradken collects Personal Information about an individual from someone else, it will take reasonable steps to ensure that the individual is or has been made aware of the matters listed in clause 7.3.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

7.4 Unsolicited Information

7.4.1 If Bradken receives personal information and did not solicit the information it will, within a reasonable period after receiving the information, determine whether or not it could have collected the information under APP-3 if Bradken had solicited the information.

7.4.2 Bradken may use or disclose the personal information for the purposes of making the determination under the sub-clause 7.4.1.

7.4.3 If Bradken determines that it could not have collected the personal information and the information is not contained in a Commonwealth record it must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

7.4.4 If sub-clause 7.4.3 does not apply in relation to the personal information, APP-5 to APP-13 apply in

relation to the information as if Bradken had collected the information under APP-3.

7.5 Notification

If Bradken collects personal information about an individual, it will take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters referred to as are reasonable in the circumstances or to otherwise ensure that the individual is aware of any such matters.

7.6 Use and Disclosure

7.6.1 Bradken will not use or disclose Personal Information about an individual for a secondary purpose under the following circumstances:

(a) unless the secondary purpose is related to the primary purpose of collection and, if the Personal Information is Sensitive Information, directly related to the primary purpose of collection or the individual would reasonably expect Bradken to use or disclose the information for the secondary purpose;

(b) the individual has consented to the use or disclosure;

(c) the information is not Sensitive Information and the use of the information is for the secondary purpose of direct marketing;

(d) the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics relevant to public health or public safety;

(e) Bradken reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety or a serious threat to public health or public safety;

(f) Bradken has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the Personal Information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(g) disclosure is required or authorised by or under law; or

(h) Bradken reasonably believes that the use or disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences.

7.6.2 If Bradken uses or discloses Personal Information under clause 7.2.1(h), it will make a written note of the use or disclosure.

7.7 Direct Marketing

7.7.1 If Bradken holds personal information about an individual, it will not use or disclose the information for the purpose of direct marketing.

7.7.2 Bradken may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if it collected the information from the individual and the individual would reasonably expect Bradken to use or disclose the information for that purpose.

7.7.3 Bradken will provide a simple means by which an individual may easily request not to receive direct marketing communications from it and an individual has not made such a request.

7.7.4 Bradken may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

7.8 Cross-Border Disclosure

Bradken may transfer Personal Information about an individual to someone (other than Bradken or the individual) who is in a foreign country only if:

(a) Bradken reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles;

(b) the individual consents to the transfer;

(c) the transfer is necessary for the performance of a contract between the individual and Bradken, or for the implementation of pre-contractual measures taken in response to the individual's request;

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between Bradken and a third party;

(e) the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual to that transfer or if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) Bradken has taken reasonable steps to ensure that the information, which it has transferred, will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

7.9 Government-related Identifiers

7.9.1 Bradken will not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.9.2 Bradken will not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in clause 7.7.1, unless:

(a) the use or disclosure is necessary for Bradken to fulfil its obligations to the agency;

(b) one or more of clauses 7.2.1(e) to (h) inclusive apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

7.9.3 In this clause:

identifier includes a number assigned by Bradken to an individual to identify uniquely the individual for the purposes of Bradken's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an *identifier*.

7.10 Data Quality

Bradken will take reasonable steps to make sure that the Personal Information it collects, uses or discloses is accurate, complete and up-to-date.

7.11 Security

7.11.1 Bradken will take reasonable steps to protect the Personal Information it holds, from misuse and loss, and from unauthorised access, modification or disclosure.

7.11.2 Bradken will take reasonable steps to destroy or permanently de-identify Personal Information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP-2.

7.12 Access

7.12.1 If Bradken holds Personal Information about an individual, it will provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of Personal Information other than health information, providing access would pose a serious and imminent threat to the life or health of any individual;

(b) in the case of health information, providing access would pose a serious threat to the life or health of any individual;

(c) providing access would have an unreasonable impact upon the privacy of other individuals;

(d) the request for access is frivolous or vexatious;

(e) the information relates to existing or anticipated legal proceedings between Bradken and the individual, and the information would not be accessible by the process of discovery in those proceedings;

(f) providing access would reveal the intentions of Bradken in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(g) providing access would be unlawful;

(h) denying access is required or authorised by or under law;

(i) providing access would be likely to prejudice an investigation of possible unlawful activity;

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks Bradken not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

7.12.2 However, where providing access would reveal evaluative information generated within Bradken about a commercially sensitive decision-making process, Bradken may explain the commercially sensitive decision rather than direct access to the information.

7.12.3 If Bradken is not required to provide the individual with access to the information because of one or more of clause 7.6.1(a) to (k) inclusive, Bradken will, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

7.13 Correction

7.13.1 Where Bradken holds Personal Information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, Bradken will take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

7.13.2 If the individual and Bradken disagree about whether the information is accurate, complete and up-to-date, and the individual asks Bradken to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, Bradken will take reasonable steps to do so.

7.13.3 Bradken will provide reasons for denial of access or a refusal to correct Personal Information.

8.0 REFERENCE DOCUMENTATION

Privacy Amendment Act 2000 http://www.austlii.edu.au/au/legis/cth/num_act/pasa2000n1552000373/